FROM CONCEPT TO REALITY – HOW TO VALIDATE SECURITY MODELS

April 26, 2023•Rita L. Griffith, CISA, CFE • Sean D. Goodwin, GSE

INTRODUCTION

RITA L. GRIFFITH CISA, CFE

Senior Manager, IT Assurance
RGriffith@wolfandco.com
617.261.8185

SEAN D. GOODWIN, GSE

Senior Manager, DenSecure
SDGoodwin@wolfandco.com
617.261.8139

AGENDA

- What is a Model?
- Differentiating Between Models vs. Tools
- “What Systems are Models?"
- Supervisory Guidance
- Sample Validation Process
- Threat Emulation Concepts
- Demonstration of Validation Process Steps
- A Little About Us

WHAT IS A MODEL?

WHAT IS A MODEL?

- As defined by SR11-7: Guidance on Model Risk Management:

A quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates.

MODEL TEST

Component Test

- Information input component
- Processing component
- Reporting component

Estimate Test

- Quantitative estimates
- Transforms inputs into outputs of a different type
- Apply statistical, economic, financial, behavioral or mathematical theories or techniques

Relationship Test

- A simplified representation of real-world relationships

Subjectivity Test

- Subjective judgment exercised at various stages of model development, implementation, use and validation

Use Test

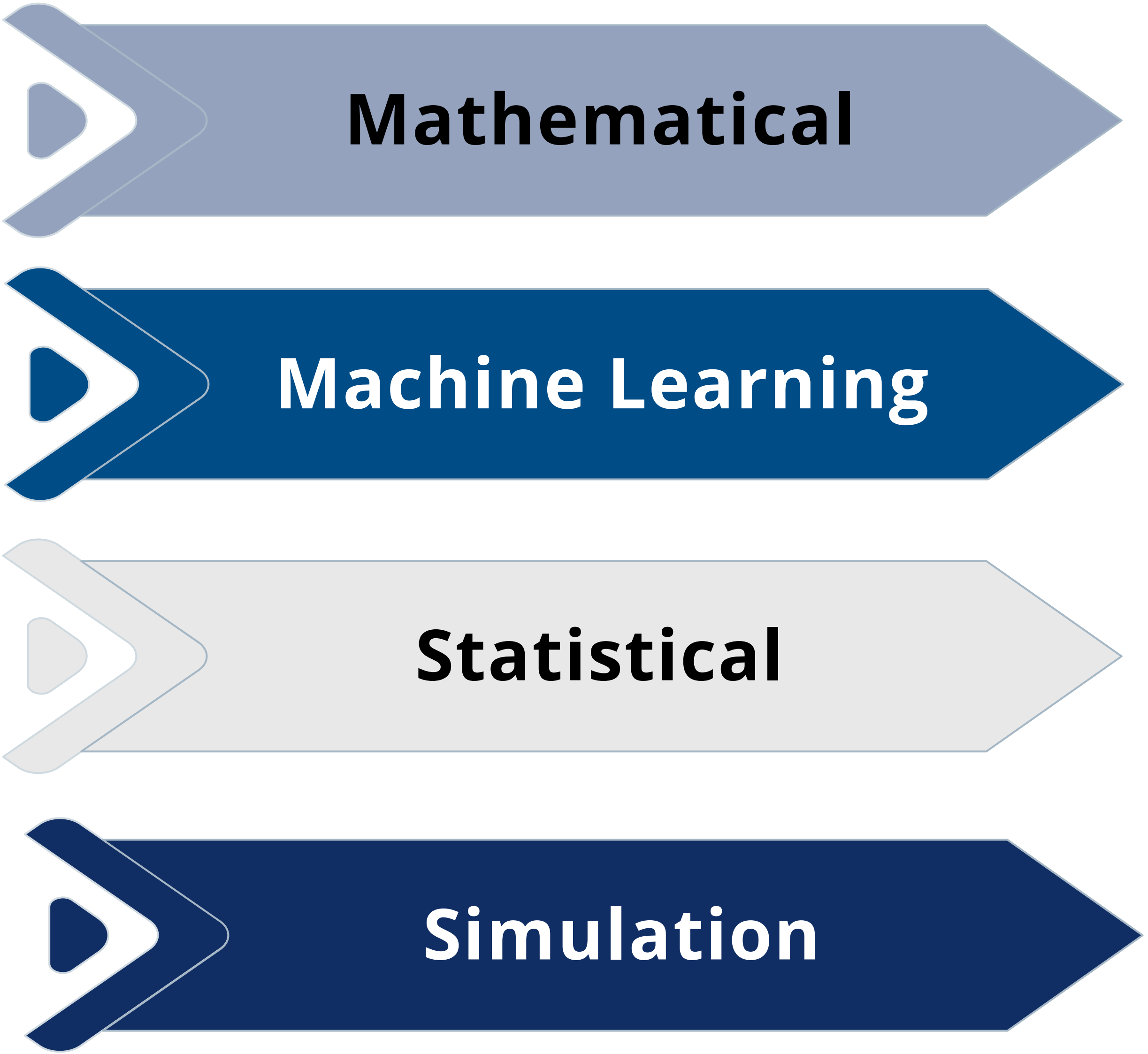
- Supports decision making and to provide predictive information in a number of business areas

WHAT IS A TOOL?

A computational process as opposed to a quantitative system. It applies simple arithmetic calculations not expected to produce ambiguous values regardless of the complexity of the computation. A tool performs simple calculations, compiles financial information, reports results but not predictive in nature.

SYSTEMS AS MODELS

SYSTEMS AS MODELS



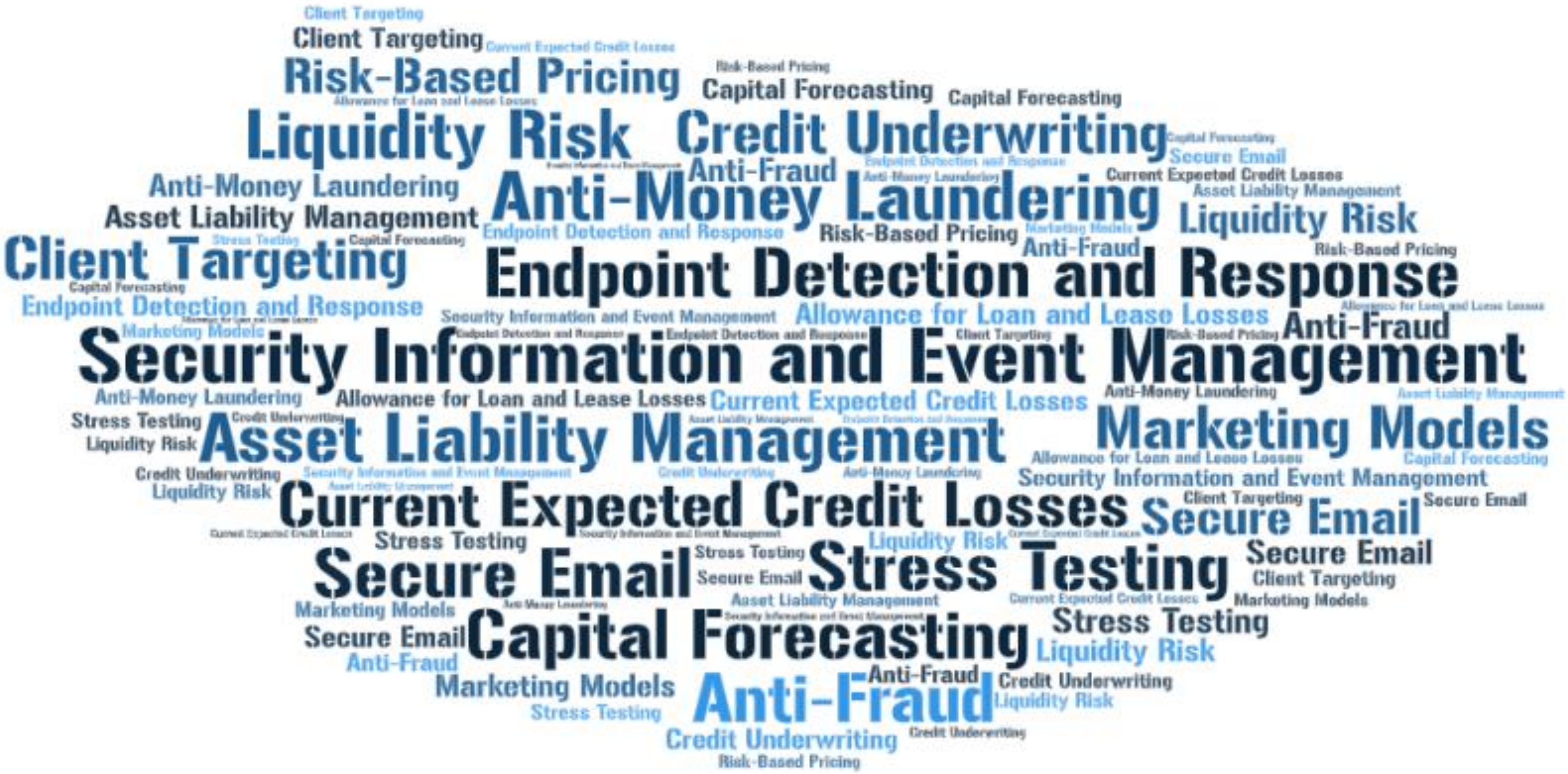
Mathematical

Machine Learning

Statistical

Simulation

SYSTEMS AS MODELS



WHAT IS MODEL RISK?

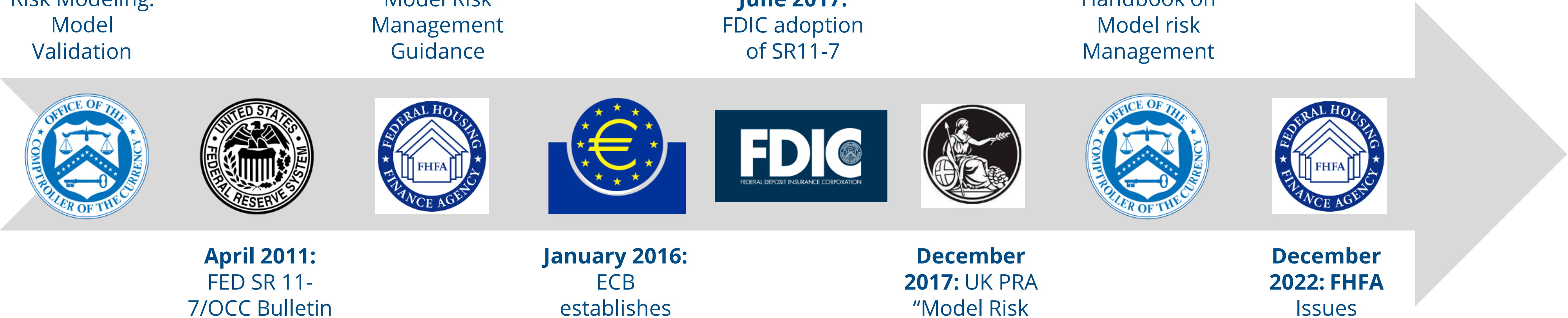
WHAT IS MODEL RISK?

- The potential for adverse consequences from decisions based on incorrect or misused model outputs and reports.

- Can lead to:
  - Financial Loss
  - Poor business and strategic decision making
  - Damage to an Institution's Reputation

REGULATORY GUIDANCE

REGULATIONS RELATING TO MODEL RISK MANAGEMENT



May 2000: OCC 2000-16 Risk Modeling: Model Validation

April 2011: FED SR 11-7/OCC Bulletin 2011-12 “Supervisory Guidance on Model Risk Management”

November 2013: FHFA Releases AB 2013-07 Model Risk Management Guidance

January 2016: ECB establishes Targeted Review of Internal Models (TRIM)

June 2017: FDIC adoption of SR11-7

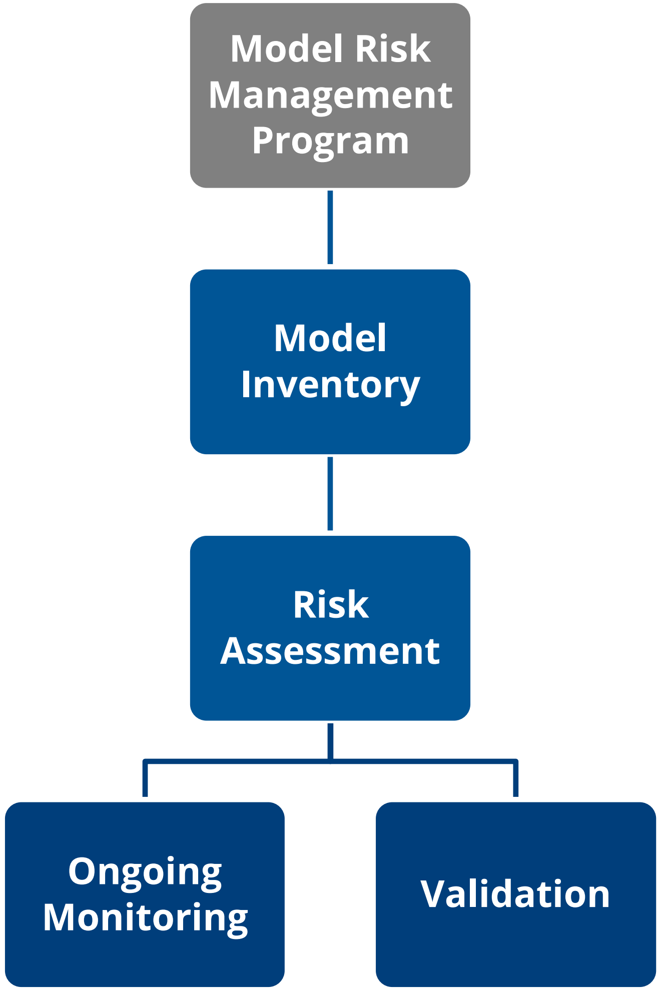
December 2017: UK PRA “Model Risk Management Principles for Stress Testing”

August 2021: OCC issues Comptroller’s Handbook on Model risk Management

December 2022: FHFA Issues Supplemental Guidance to Model Risk Management Guidance

COMPONENTS OF EFFECTIVE MODEL RISK MANAGEMENT

COMPONENTS OF EFFECTIVE MODEL RISK MANAGEMNET



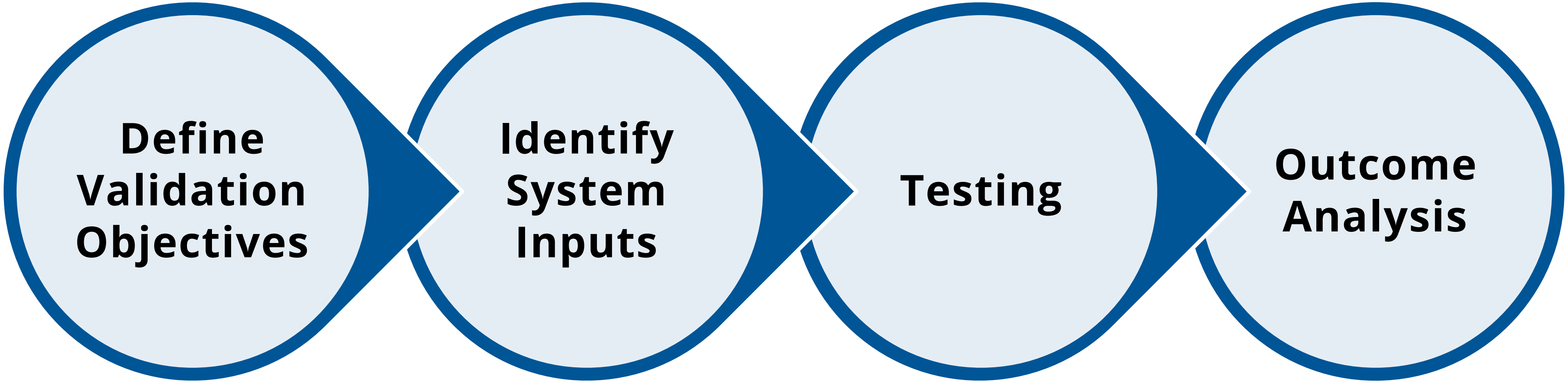
WHAT IS A MODEL VALIDATION?

WHAT IS A MODEL VALIDATION?

A set of processes and activities intended to verify that the models are performing as expected and are in line with their design objectives and business uses.

SAMPLE VALIDATION PROCESS

SAMPLE VALIDATION PROCESS



THREAT EMULATION TO VALIDATE MODELS

THREAT EMULATION

- Gather Cyber Threat Intelligence
  - Verizon DBIR, US-CERT alerts, etc.
- Identify Procedures to Emulate
- Identify Metrics
  - Data Sources, Detections, Response times
- Execution
  - May start with Tabletop Exercise (TTX)
- Lessons Learned
  - Critical to feed into the next cycle of testing

MITRE ATT&CK®

- Tracks threat actors through observable data
- Tactics, Techniques, and Procedures (TTPs)
- Post compromise focus

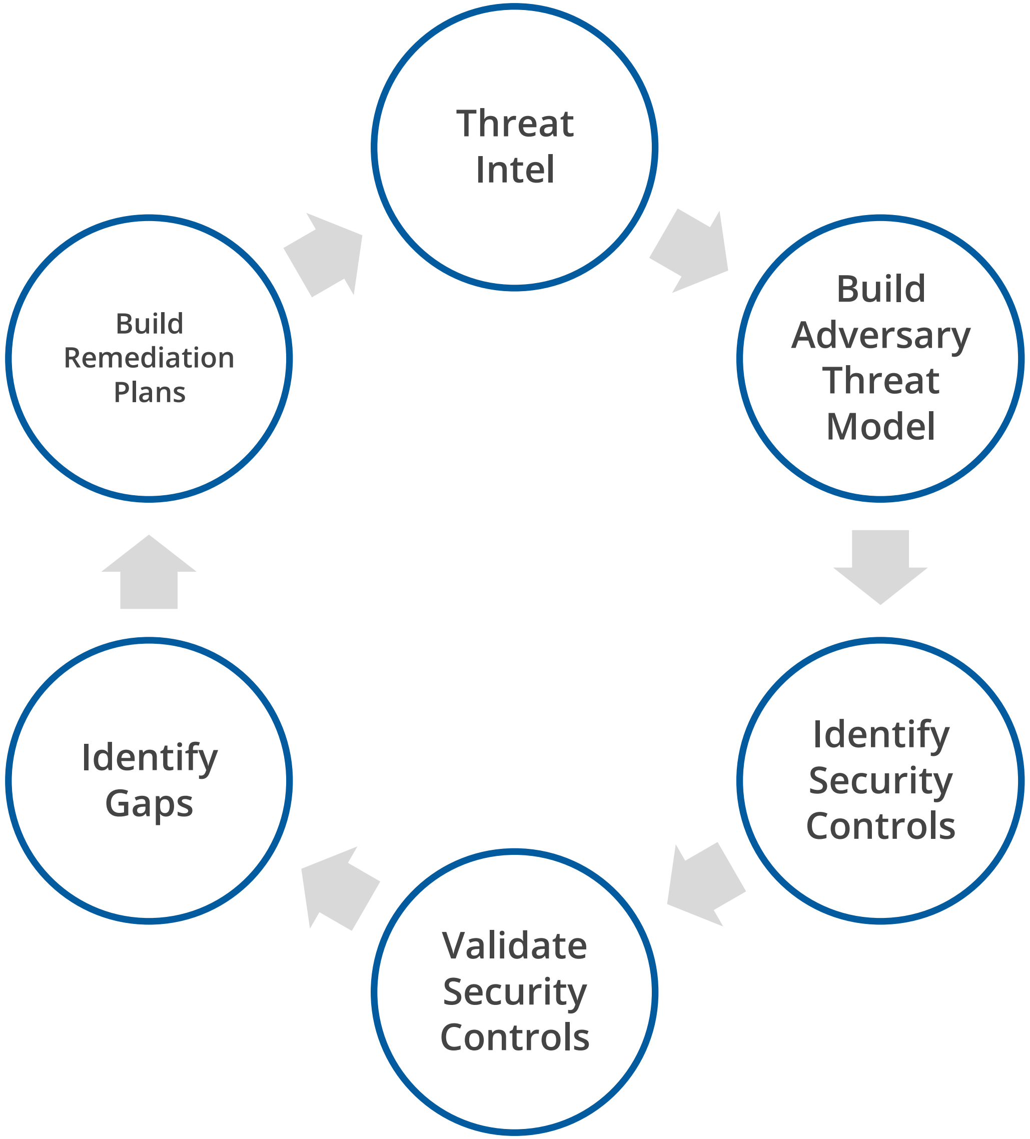
MITRE ATT&CK® MATRICES

MATRIX	ENTERPRISE	MOBILE	INDUSTRIAL CONTROL SYSTEMS (ISC)
Platforms:	Windows macOS Linux PRE Azure AD Office 365 Google Workspace SaaS IaaS Network Containers	Android iOS	ICS networks
Tactics:	14	14	12
Techniques:	379	92	78

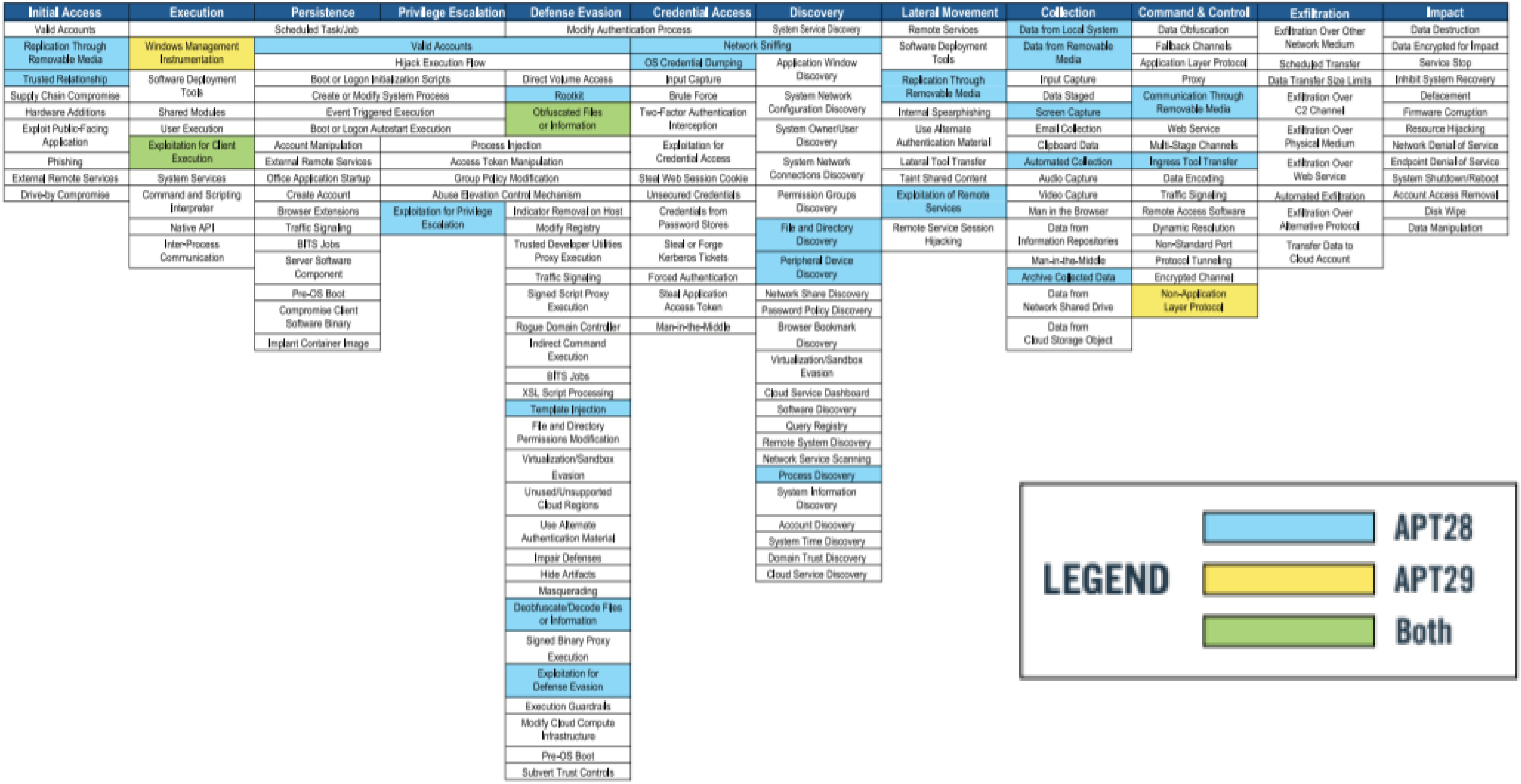
HOW MITRE ATT&CK® CAN BE USED

Outputs

- Threat model(s) of adversary tactics and techniques
- Mitigation and detection capabilities in place
- Testing plan to validate controls
- Remediation plans
- Board & Executive roadmap


Threat Intel
Build Adversary Threat Model
Identify Security Controls
Validate Security Controls
Identify Gaps
Build Remediation Plans

USE ATT&CK FOR CYBER THREAT INTELLIGENCE



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command & Control	Exfiltration	Impact
Valid Accounts	Scheduled Task/Job			Modify Authentication Process		System Service Discovery	Remote Services	Data from Local System 🟦	Data Obfuscation	Exfiltration Over Other Network Medium	Data Destruction
Replication Through Removable Media 🟦	Windows Management Instrumentation 🟨	Valid Accounts 🟦			Network Sniffing 🟦		Software Deployment Tools	Data from Removable Media 🟦	Fallback Channels		Data Encrypted for Impact
		Hijack Execution Flow			OS Credential Dumping 🟦	Application Window Discovery			Application Layer Protocol	Scheduled Transfer	Service Stop
Trusted Relationship 🟦	Software Deployment Tools	Boot or Logon Initialization Scripts		Direct Volume Access	Input Capture		Replication Through Removable Media 🟦	Input Capture	Proxy	Data Transfer Size Limits	Inhibit System Recovery
Supply Chain Compromise		Create or Modify System Process		Rootkit 🟦	Brute Force	System Network Configuration Discovery		Data Staged	Communication Through Removable Media 🟦	Exfiltration Over C2 Channel	Defacement
Hardware Additions	Shared Modules	Event Triggered Execution		Obfuscated Files or Information 🟩	Two-Factor Authentication Interception		Internal Spearphishing	Screen Capture 🟦			Firmware Corruption
Exploit Public-Facing Application	User Execution	Boot or Logon Autostart Execution				System Owner/User Discovery	Use Alternate Authentication Material	Email Collection	Web Service	Exfiltration Over Physical Medium	Resource Hijacking
	Exploitation for Client Execution 🟩	Account Manipulation	Process Injection		Exploitation for Credential Access			Clipboard Data	Multi-Stage Channels		Network Denial of Service
Phishing		External Remote Services	Access Token Manipulation			System Network Connections Discovery	Lateral Tool Transfer	Automated Collection 🟦	Ingress Tool Transfer 🟦	Exfiltration Over Web Service	Endpoint Denial of Service
External Remote Services	System Services	Office Application Startup	Group Policy Modification		Steal Web Session Cookie		Taint Shared Content	Audio Capture	Data Encoding		System Shutdown/Reboot
Drive-by Compromise	Command and Scripting Interpreter	Create Account	Abuse Elevation Control Mechanism		Unsecured Credentials	Permission Groups Discovery	Exploitation of Remote Services 🟦	Video Capture	Traffic Signaling	Automated Exfiltration	Account Access Removal
		Browser Extensions	Exploitation for Privilege Escalation 🟦	Indicator Removal on Host	Credentials from Password Stores			Man in the Browser	Remote Access Software	Exfiltration Over Alternative Protocol	Disk Wipe
	Native API	Traffic Signaling		Modify Registry		File and Directory Discovery 🟦	Remote Service Session Hijacking	Data from Information Repositories	Dynamic Resolution		Data Manipulation
	Inter-Process Communication	BITS Jobs		Trusted Developer Utilities Proxy Execution	Steal or Forge Kerberos Tickets				Non-Standard Port	Transfer Data to Cloud Account	
		Server Software Component				Peripheral Device Discovery 🟦		Man-in-the-Middle	Protocol Tunneling		
				Traffic Signaling	Forced Authentication			Archive Collected Data 🟦	Encrypted Channel		
		Pre-OS Boot		Signed Script Proxy Execution	Steal Application Access Token	Network Share Discovery		Data from Network Shared Drive	Non-Application Layer Protocol 🟨		
		Compromise Client Software Binary				Password Policy Discovery					
				Rogue Domain Controller	Man-in-the-Middle	Browser Bookmark Discovery		Data from Cloud Storage Object			
		Implant Container Image		Indirect Command Execution		Virtualization/Sandbox Evasion					
				BITS Jobs							
				XSL Script Processing		Cloud Service Dashboard					
				Template Injection 🟦		Software Discovery					
				File and Directory Permissions Modification		Query Registry					
						Remote System Discovery					
				Virtualization/Sandbox Evasion		Network Service Scanning					
						Process Discovery 🟦					
				Unused/Unsupported Cloud Regions		System Information Discovery					
				Use Alternate Authentication Material		Account Discovery					
						System Time Discovery					
				Impair Defenses		Domain Trust Discovery					
				Hide Artifacts		Cloud Service Discovery					
				Masquerading							
				Deobfuscate/Decode Files or Information 🟦							
				Signed Binary Proxy Execution							
				Exploitation for Defense Evasion 🟦							
				Execution Guardrails							
				Modify Cloud Compute Infrastructure							
				Pre-OS Boot							
				Subvert Trust Controls							

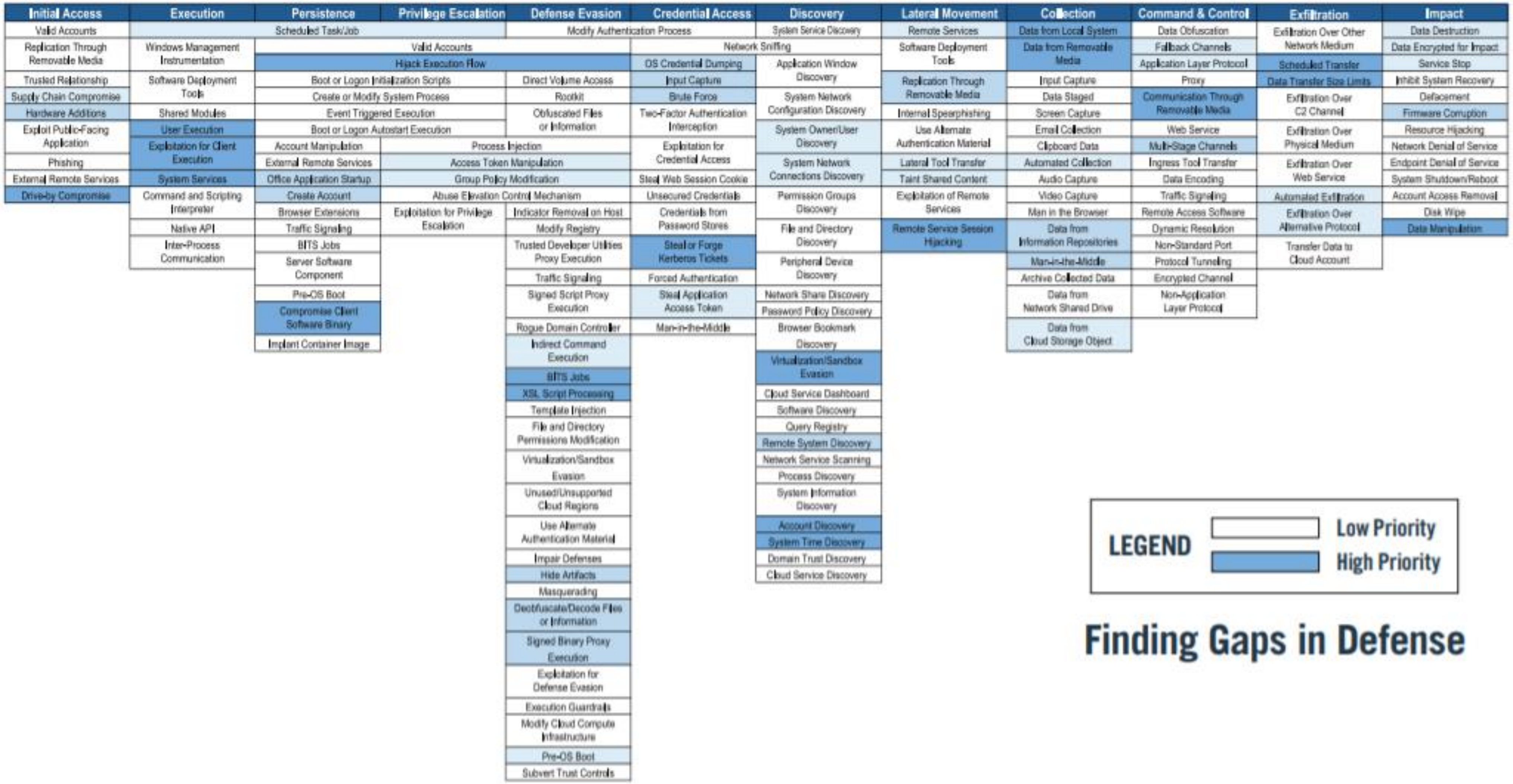
LEGEND

🟦 APT28

🟨 APT29

🟩 Both

USE ATT&CK TO BUILD YOUR DEFENSIVE PLATFORM



Initial Access
- Valid Accounts
- Replication Through Removable Media
- Trusted Relationship
- Supply Chain Compromise
- Hardware Additions
- Exploit Public-Facing Application
- Phishing
- External Remote Services
- Drive-by Compromise

Execution
- Scheduled Task/Job
- Windows Management Instrumentation
- Software Deployment Tools
- Shared Modules
- User Execution
- Exploitation for Client Execution
- System Services
- Command and Scripting Interpreter
- Native API
- Inter-Process Communication

Persistence
- Scheduled Task/Job
- Valid Accounts
- Hijack Execution Flow
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Event Triggered Execution
- Boot or Logon Autostart Execution
- Account Manipulation
- External Remote Services
- Office Application Startup
- Create Account
- Browser Extensions
- Traffic Signaling
- BITS Jobs
- Server Software Component
- Pre-OS Boot
- Compromise Client Software Binary
- Implant Container Image

Privilege Escalation
- Scheduled Task/Job
- Valid Accounts
- Hijack Execution Flow
- Boot or Logon Initialization Scripts
- Create or Modify System Process
- Event Triggered Execution
- Boot or Logon Autostart Execution
- Process Injection
- Access Token Manipulation
- Group Policy Modification
- Abuse Elevation Control Mechanism
- Exploitation for Privilege Escalation

Defense Evasion
- Modify Authentication Process
- Valid Accounts
- Hijack Execution Flow
- Direct Volume Access
- Rootkit
- Obfuscated Files or Information
- Process Injection
- Access Token Manipulation
- Group Policy Modification
- Abuse Elevation Control Mechanism
- Indicator Removal on Host
- Modify Registry
- Trusted Developer Utilities Proxy Execution
- Traffic Signaling
- Signed Script Proxy Execution
- Rogue Domain Controller
- Indirect Command Execution
- BITS Jobs
- XSL Script Processing
- Template Injection
- File and Directory Permissions Modification
- Virtualization/Sandbox Evasion
- Unused/Unsupported Cloud Regions
- Use Alternate Authentication Material
- Impair Defenses
- Hide Artifacts
- Masquerading
- Deobfuscate/Decode Files or Information
- Signed Binary Proxy Execution
- Exploitation for Defense Evasion
- Execution Guardrails
- Modify Cloud Compute Infrastructure
- Pre-OS Boot
- Subvert Trust Controls

Credential Access
- Modify Authentication Process
- Network Sniffing
- OS Credential Dumping
- Input Capture
- Brute Force
- Two-Factor Authentication Interception
- Exploitation for Credential Access
- Steal Web Session Cookie
- Unsecured Credentials
- Credentials from Password Stores
- Steal or Forge Kerberos Tickets
- Forced Authentication
- Steal Application Access Token
- Man-in-the-Middle

Discovery
- System Service Discovery
- Network Sniffing
- Application Window Discovery
- System Network Configuration Discovery
- System Owner/User Discovery
- System Network Connections Discovery
- Permission Groups Discovery
- File and Directory Discovery
- Peripheral Device Discovery
- Network Share Discovery
- Password Policy Discovery
- Browser Bookmark Discovery
- Virtualization/Sandbox Evasion
- Cloud Service Dashboard
- Software Discovery
- Query Registry
- Remote System Discovery
- Network Service Scanning
- Process Discovery
- System Information Discovery
- Account Discovery
- System Time Discovery
- Domain Trust Discovery
- Cloud Service Discovery

Lateral Movement
- Remote Services
- Software Deployment Tools
- Replication Through Removable Media
- Internal Spearphishing
- Use Alternate Authentication Material
- Lateral Tool Transfer
- Taint Shared Content
- Exploitation of Remote Services
- Remote Service Session Hijacking

Collection
- Data from Local System
- Data from Removable Media
- Input Capture
- Data Staged
- Screen Capture
- Email Collection
- Clipboard Data
- Automated Collection
- Audio Capture
- Video Capture
- Man in the Browser
- Data from Information Repositories
- Man-in-the-Middle
- Archive Collected Data
- Data from Network Shared Drive
- Data from Cloud Storage Object

Command & Control
- Data Obfuscation
- Fallback Channels
- Application Layer Protocol
- Proxy
- Communication Through Removable Media
- Web Service
- Multi-Stage Channels
- Ingress Tool Transfer
- Data Encoding
- Traffic Signaling
- Remote Access Software
- Dynamic Resolution
- Non-Standard Port
- Protocol Tunneling
- Encrypted Channel
- Non-Application Layer Protocol

Exfiltration
- Exfiltration Over Other Network Medium
- Scheduled Transfer
- Data Transfer Size Limits
- Exfiltration Over C2 Channel
- Exfiltration Over Physical Medium
- Exfiltration Over Web Service
- Automated Exfiltration
- Exfiltration Over Alternative Protocol
- Transfer Data to Cloud Account

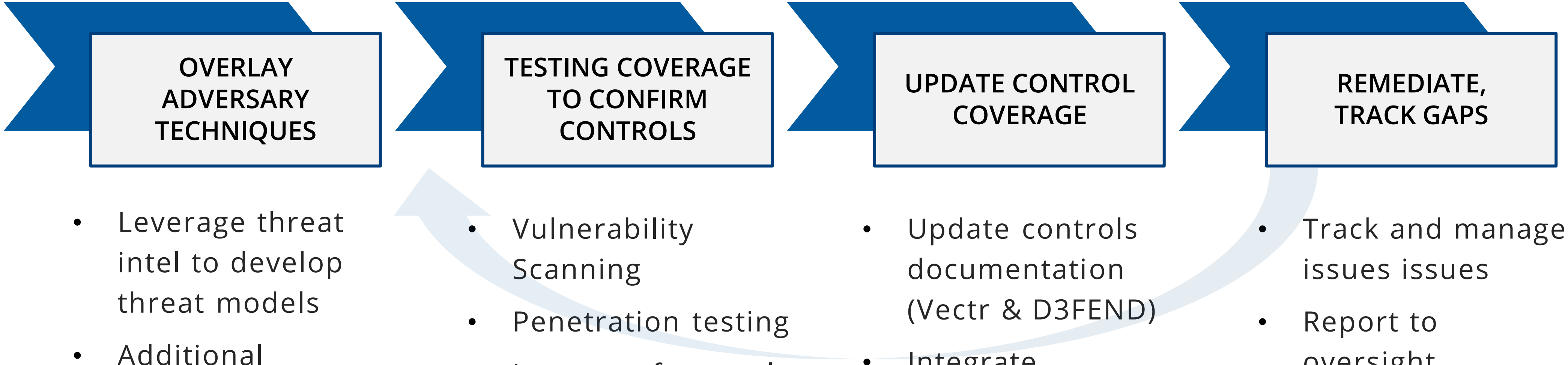
Impact
- Data Destruction
- Data Encrypted for Impact
- Service Stop
- Inhibit System Recovery
- Defacement
- Firmware Corruption
- Resource Hijacking
- Network Denial of Service
- Endpoint Denial of Service
- System Shutdown/Reboot
- Account Access Removal
- Disk Wipe
- Data Manipulation

LEGEND

□	Low Priority
■	High Priority

Finding Gaps in Defense

KEEP YOUR THREAT MODELS UP TO DATE



OVERLAY ADVERSARY TECHNIQUES
TESTING COVERAGE TO CONFIRM CONTROLS
UPDATE CONTROL COVERAGE
REMEDIATE, TRACK GAPS

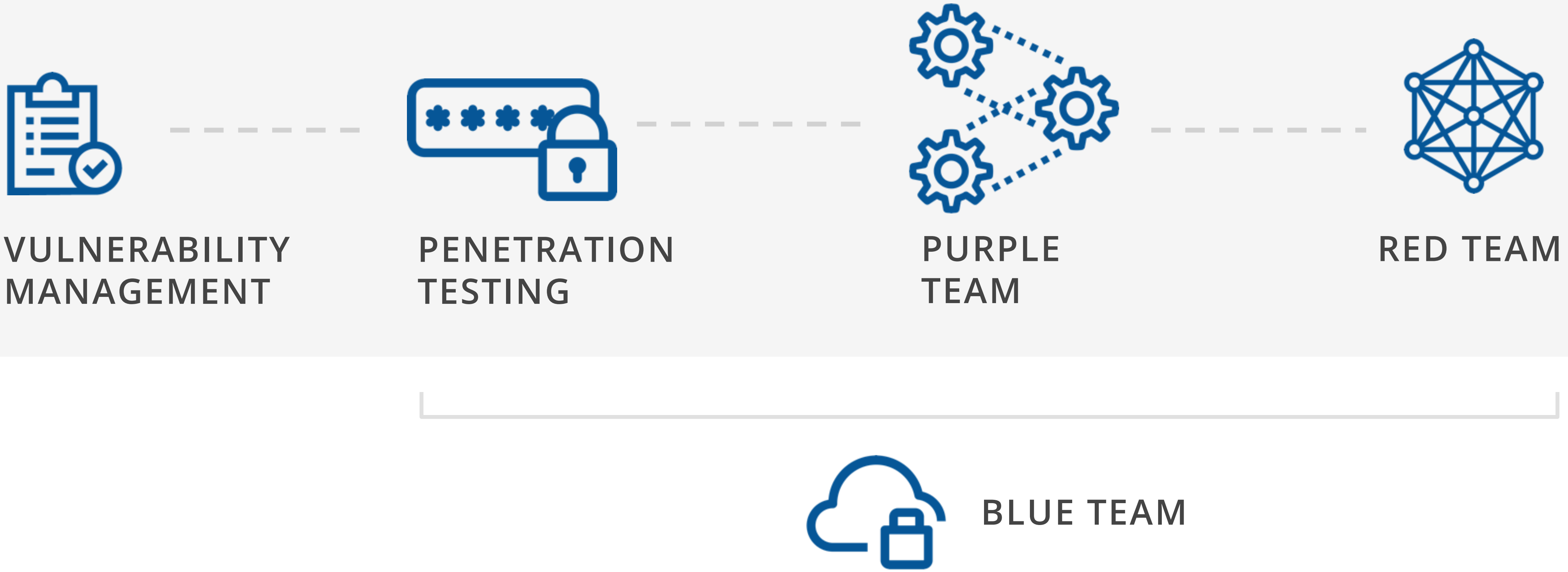
- Leverage threat intel to develop threat models
- Additional adversaries
- New techniques observed by existing adversaries
- Overlay controls

- Vulnerability Scanning
- Penetration testing
- Leverage free tools such as Atomic Red Team, Invoke-Atomic, & CALDERA
- Purple team / blue team exercises (tools such as Vectr and MITRE D3FEND)

- Update controls documentation (Vectr & D3FEND)
- Integrate documentation into processes

- Track and manage issues issues
- Report to oversight committee / board

CYBERSECURITY TESTING & RESPONSE MATURITY



VULNERABILITY MANAGEMENT

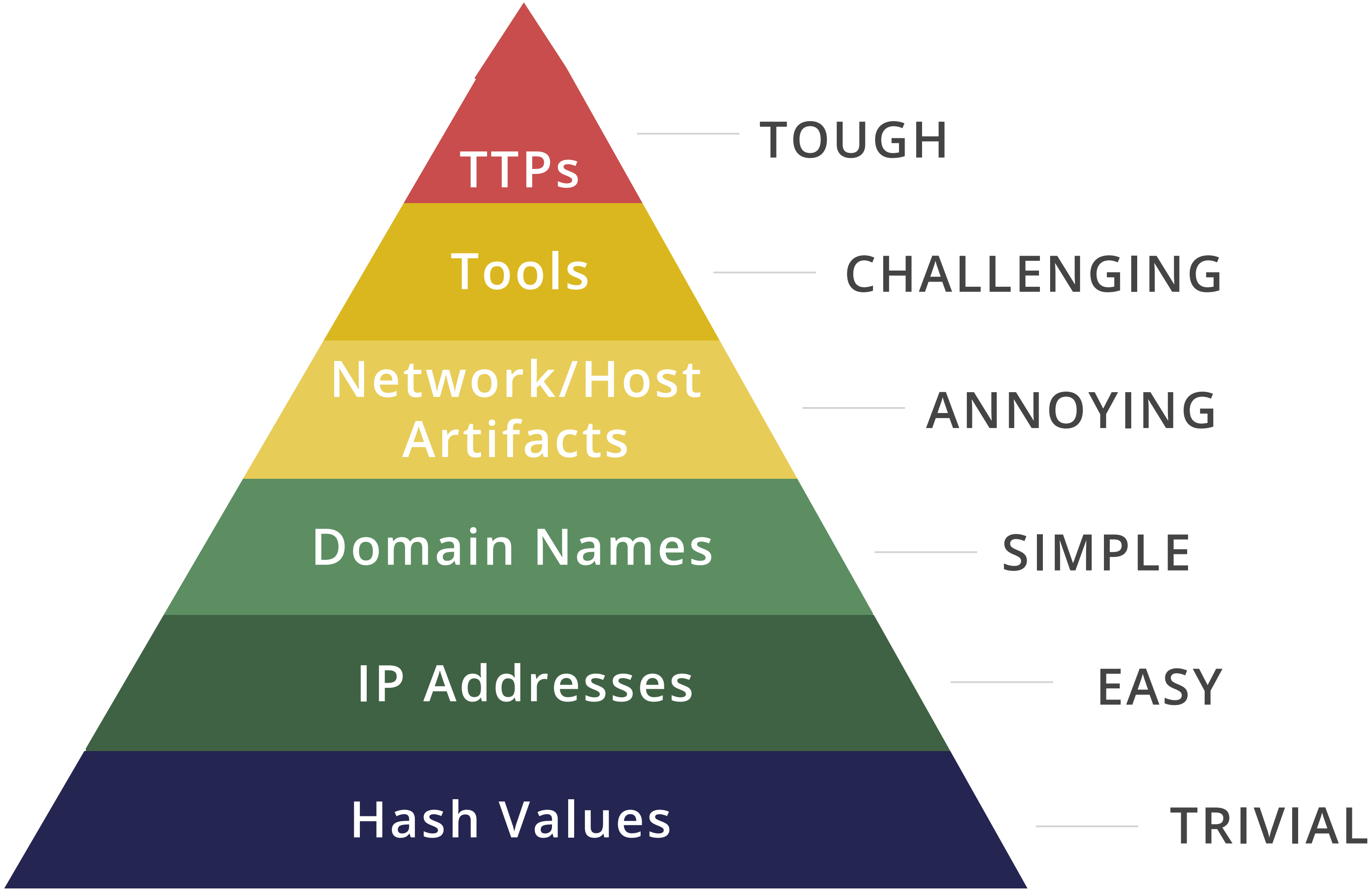
PENETRATION TESTING

PURPLE TEAM

RED TEAM

BLUE TEAM

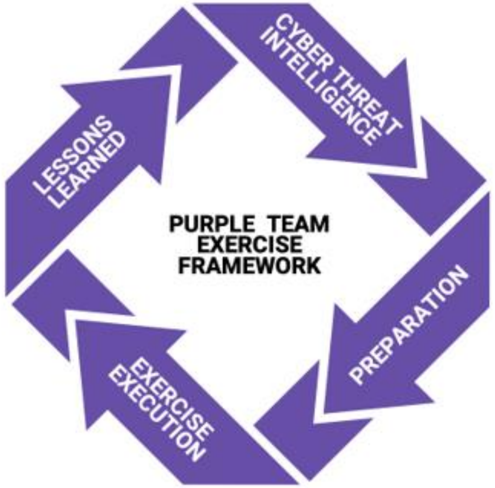
BREAKING THE CHAIN

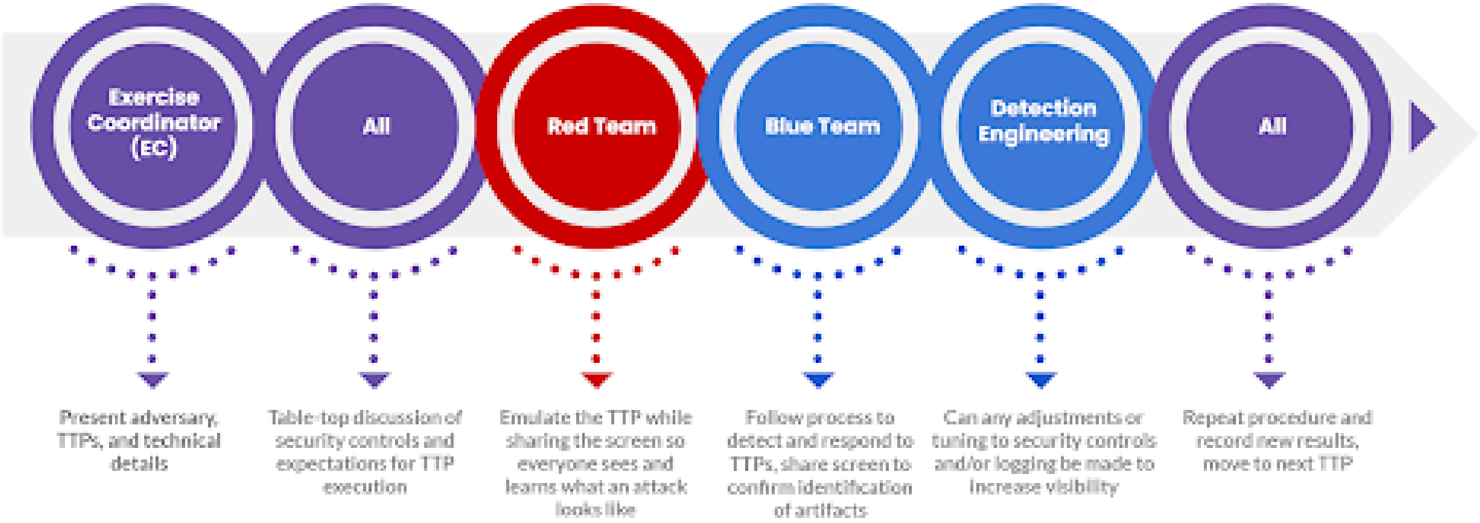


Source: https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html

THREAT EMULATION MAKE A PLAN

- Plan for the long-term success
- Iteration is key – get processes in place before looking to smash a home run
- PTES outlines procedural support for this program
  - Start with a TTX to introduce terms and approach





Present adversary, TTPs, and technical details

Table-top discussion of security controls and expectations for TTP execution

Emulate the TTP while sharing the screen so everyone sees and learns what an attack looks like

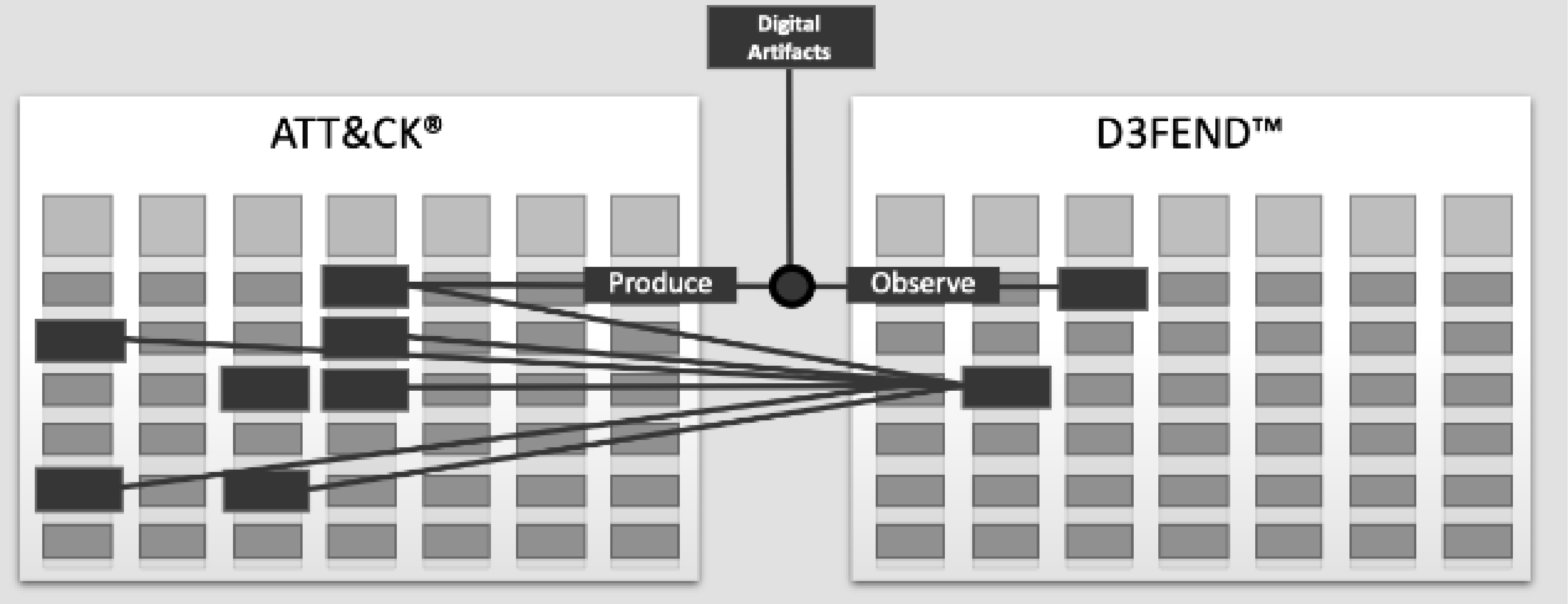
Follow process to detect and respond to TTPs, share screen to confirm identification of artifacts

Can any adjustments or tuning to security controls and/or logging be made to increase visibility

Repeat procedure and record new results, move to next TTP

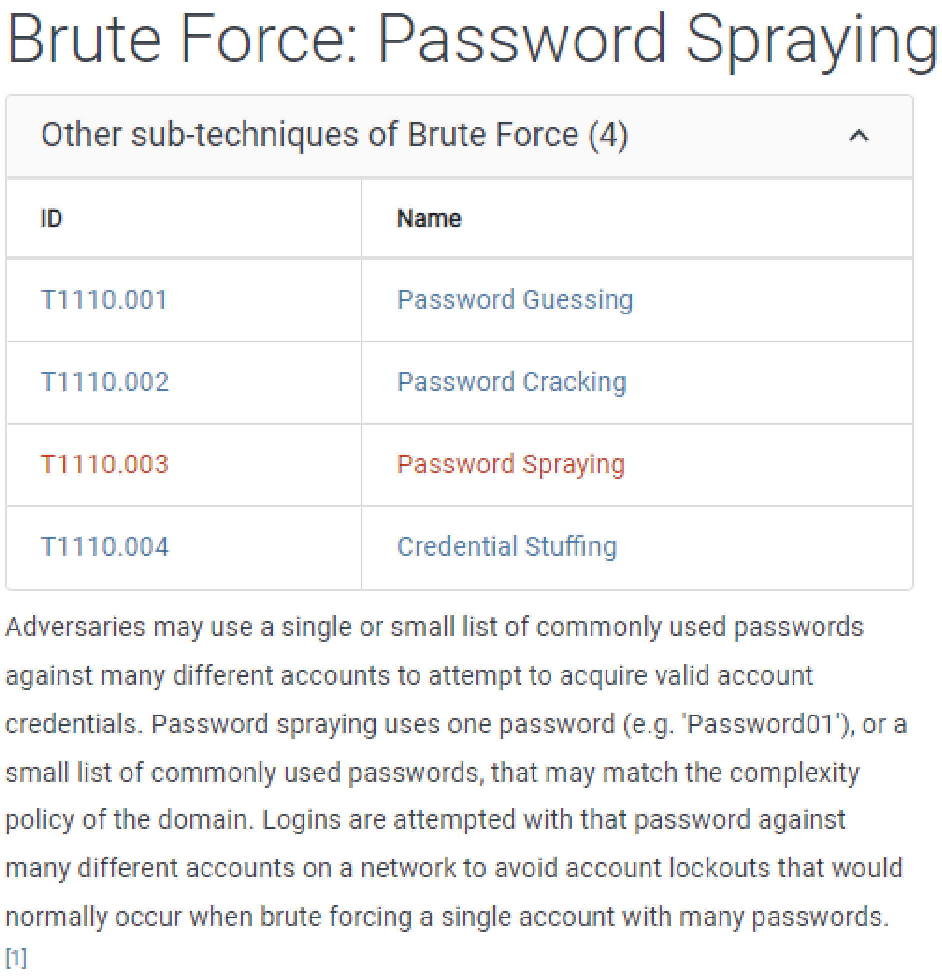
https://github.com/scythe-io/purple-team-exercise-framework

THREAT EMULATION – REMEDIATION



Simplified Offensive and Defensive Technique Relationships

REMEDIATION – PASSWORD SPRAY

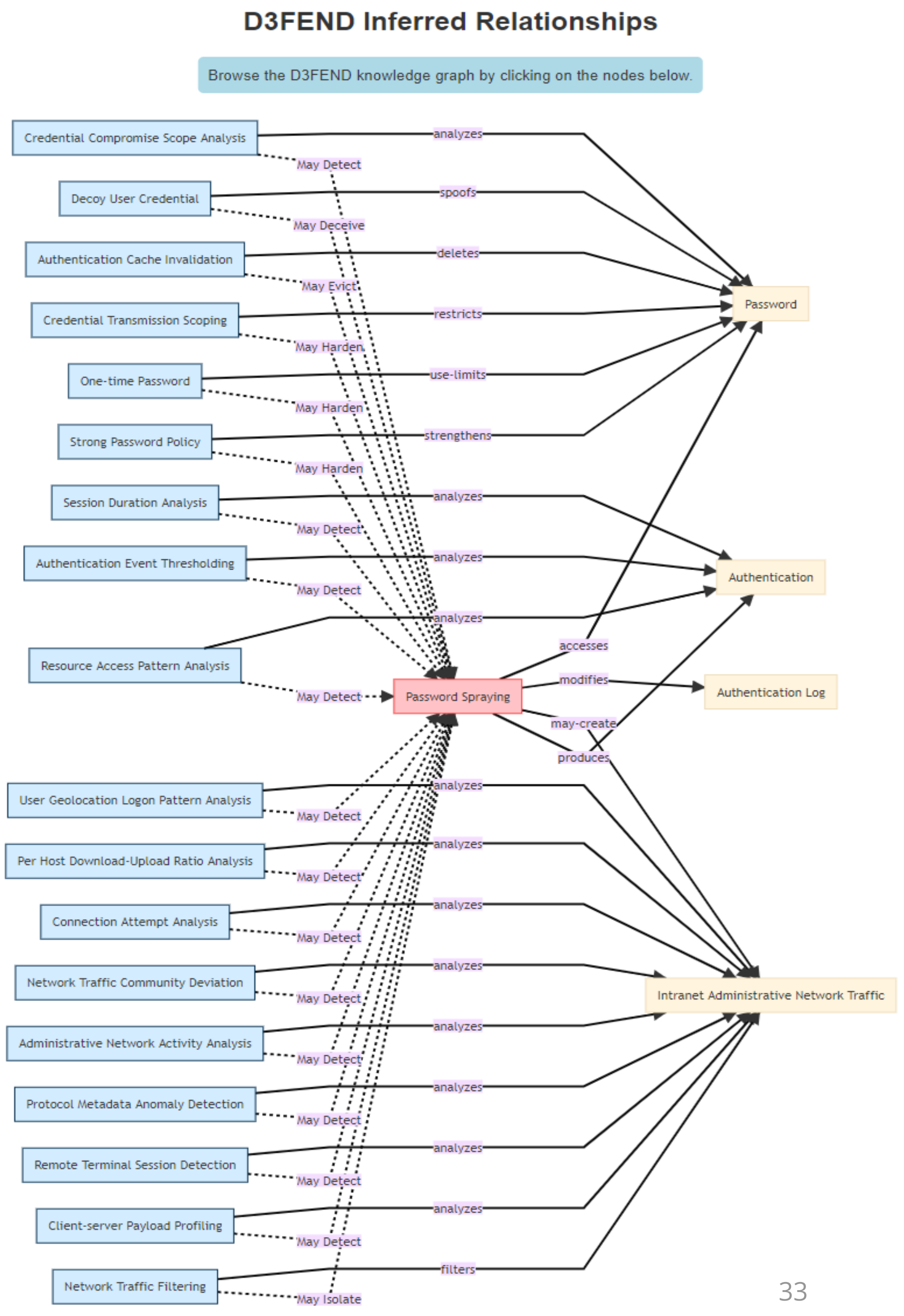


Brute Force: Password Spraying

Other sub-techniques of Brute Force (4)

ID	Name
T1110.001	Password Guessing
T1110.002	Password Cracking
T1110.003	Password Spraying
T1110.004	Credential Stuffing

Adversaries may use a single or small list of commonly used passwords against many different accounts to attempt to acquire valid account credentials. Password spraying uses one password (e.g. 'Password01'), or a small list of commonly used passwords, that may match the complexity policy of the domain. Logins are attempted with that password against many different accounts on a network to avoid account lockouts that would normally occur when brute forcing a single account with many passwords. [1]



D3FEND Inferred Relationships

Browse the D3FEND knowledge graph by clicking on the nodes below.

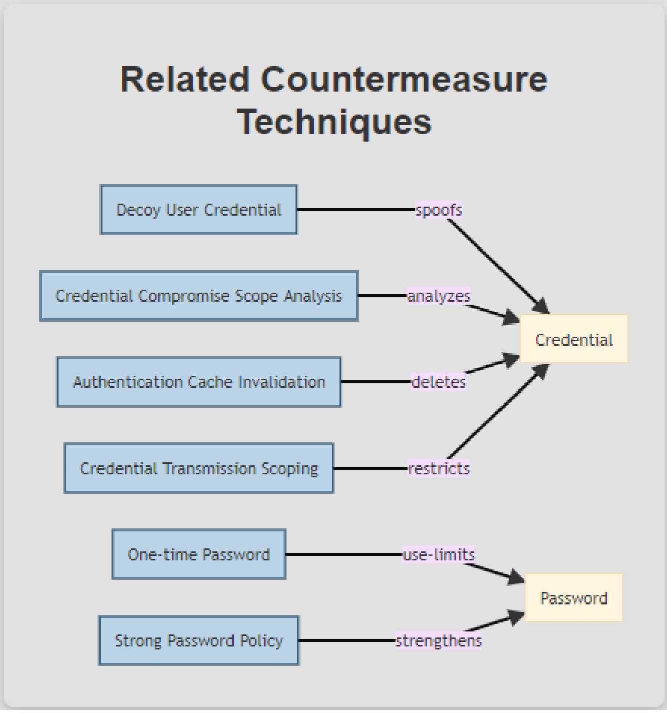
Credential Compromise Scope Analysis – analyzes – May Detect
Decoy User Credential – spoofs – May Deceive
Authentication Cache Invalidation – deletes – May Evict
Credential Transmission Scoping – restricts – May Harden
One-time Password – use-limits – May Harden
Strong Password Policy – strengthens – May Harden
Session Duration Analysis – analyzes – May Detect
Authentication Event Thresholding – analyzes – May Detect
Resource Access Pattern Analysis – analyzes – May Detect
User Geolocation Logon Pattern Analysis – analyzes – May Detect
Per Host Download-Upload Ratio Analysis – analyzes – May Detect
Connection Attempt Analysis – analyzes – May Detect
Network Traffic Community Deviation – analyzes – May Detect
Administrative Network Activity Analysis – analyzes – May Detect
Protocol Metadata Anomaly Detection – analyzes – May Detect
Remote Terminal Session Detection – analyzes – May Detect
Client-server Payload Profiling – analyzes – May Detect
Network Traffic Filtering – filters – May Isolate

Password Spraying – accesses – modifies – may-create – produces

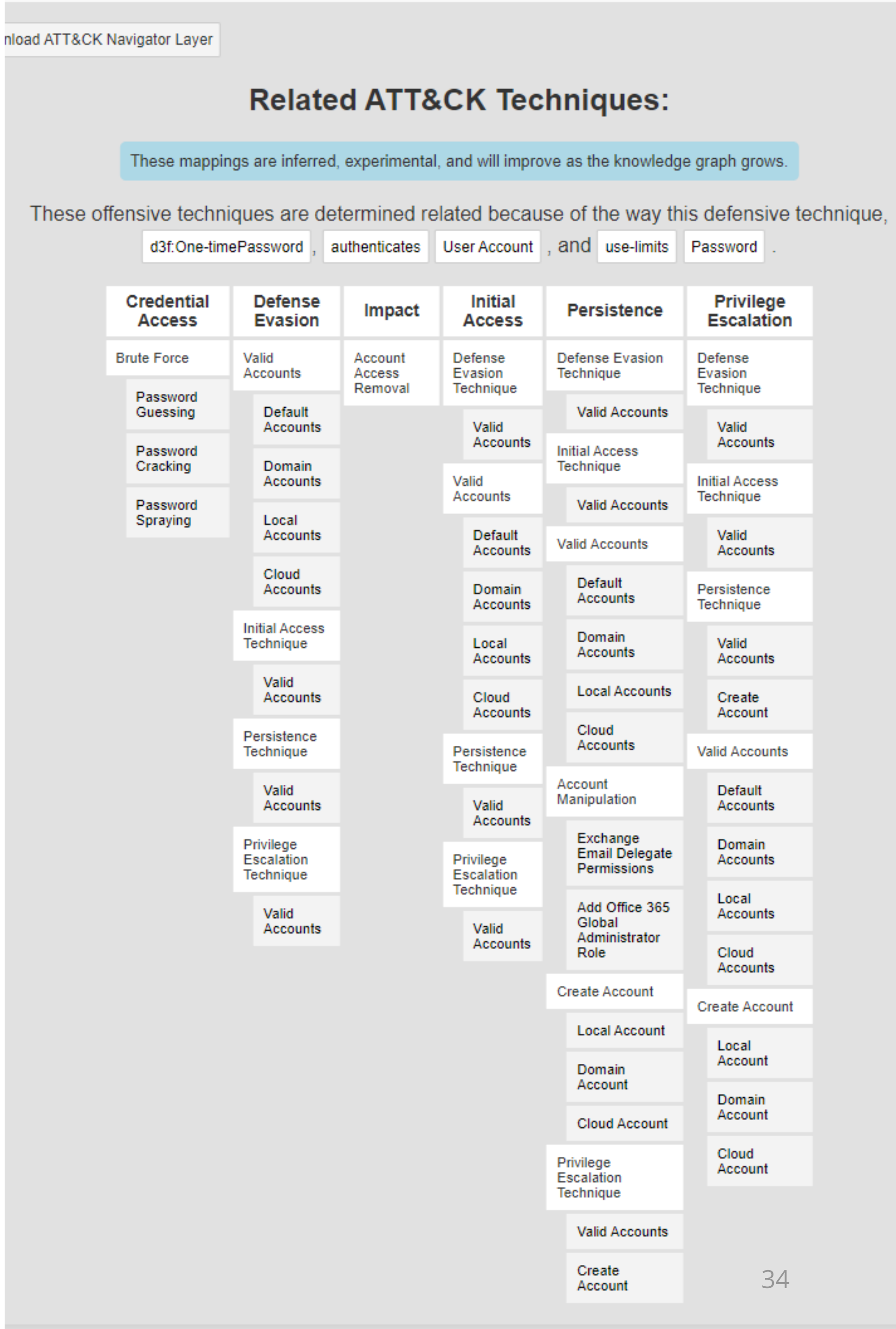
Password
Authentication
Authentication Log
Intranet Administrative Network Traffic

REMEDIATION – PASSWORD SPRAY

- Review available mitigations with efficiency in mind
- ATT&CK Navigator layers available for visual aids



Related Countermeasure Techniques



Related ATT&CK Techniques:

These mappings are inferred, experimental, and will improve as the knowledge graph grows.

These offensive techniques are determined related because of the way this defensive technique, d3f:One-timePassword , authenticates User Account , and use-limits Password .

Credential Access

- Brute Force
  - Password Guessing
  - Password Cracking
  - Password Spraying

Defense Evasion

- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts
- Initial Access Technique
  - Valid Accounts
- Persistence Technique
  - Valid Accounts
- Privilege Escalation Technique
  - Valid Accounts

Impact

- Account Access Removal

Initial Access

- Defense Evasion Technique
  - Valid Accounts
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts
- Persistence Technique
  - Valid Accounts
- Privilege Escalation Technique
  - Valid Accounts

Persistence

- Defense Evasion Technique
  - Valid Accounts
- Initial Access Technique
  - Valid Accounts
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts
- Account Manipulation
  - Exchange Email Delegate Permissions
  - Add Office 365 Global Administrator Role
- Create Account
  - Local Account
  - Domain Account
  - Cloud Account
- Privilege Escalation Technique
  - Valid Accounts
  - Create Account

Privilege Escalation

- Defense Evasion Technique
  - Valid Accounts
- Initial Access Technique
  - Valid Accounts
- Persistence Technique
  - Valid Accounts
  - Create Account
- Valid Accounts
  - Default Accounts
  - Domain Accounts
  - Local Accounts
  - Cloud Accounts
- Create Account
  - Local Account
  - Domain Account
  - Cloud Account

EXAMPLE SIEM VALIDATION

DEFINING OBJECTIVES

- What is the SIEM used for?
  - What is it NOT used for?
- What date types & sources feed into the SIEM?
- What are the threats we're concerned about?
  - Carabank APT example

GATHER AND PREPARE DATA

- Policies and Procedures
  - Logging or Monitoring
  - Incident Response
  - SIEM related checklists/runbooks
- Configurations
  - Log Sources
  - Alerts
  - Default Rules
  - Custom Rules

- Adversary TTPs
  - Identify overlap with expected controls
  - Document expected outcomes
- Test Infrastructure Creation
  - Tools
  - Network Connections
  - Execution method(s)

TEST THE SIEM SYSTEM

- Carabank TTPs
  - CTID Emulation Plan template
    - Local Discovery (T1033, T1082, T1057)
    - Screen Capture (T1113)
    - Stage 2nd stage RAT (T1112)
    - Execute 2nd stage RAT (T1012, T1055)
    - Local and Domain Discovery (T1083, T1018, T1069)

EVALUATE RESULTS

- Observability
  - Did we capture a log?
- Detection
  - Did we generate an alert?
- Mitigation
  - Did we prevent or stop the action?

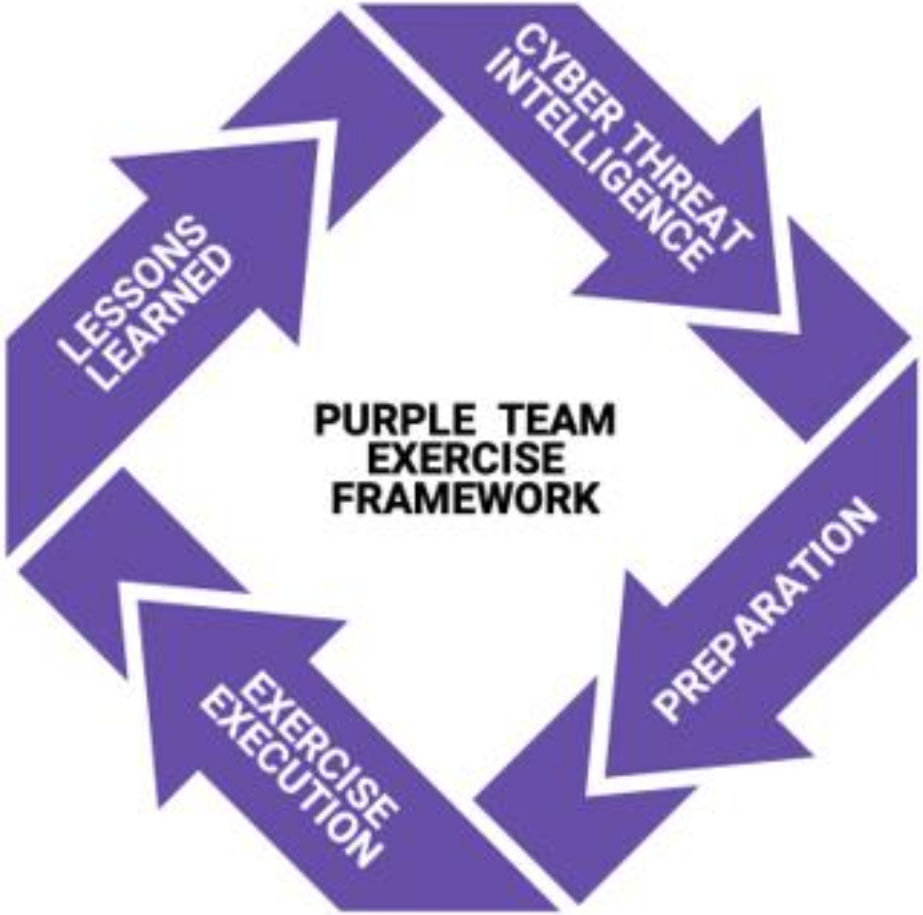
REFINE THE SIEM

- Observability
  - Did we capture a log?
    - Add logging source
    - Refine audit policies
- Detection
  - Did we generate an alert?
    - Create new alert
    - Refine alert thresholds

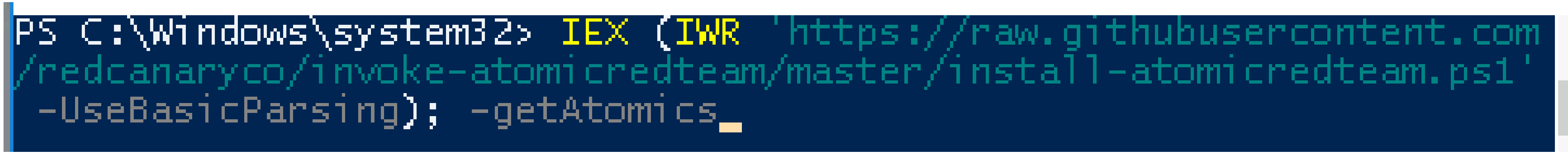
- Mitigation
  - Did we prevent or stop the action?
    - Can we prevent within acceptable F/P rates

REPEAT THE PROCESS

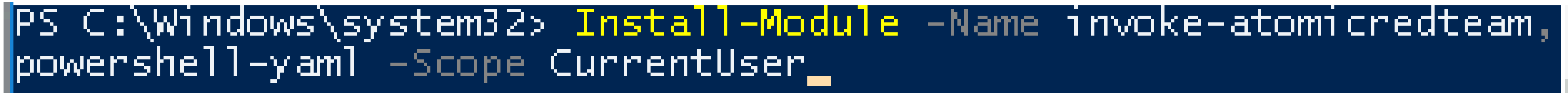
- Continue to refine the process based on your evolving threat model
- Use the process to "test" changes to controls
- Document results over time



DEMONSTRATION

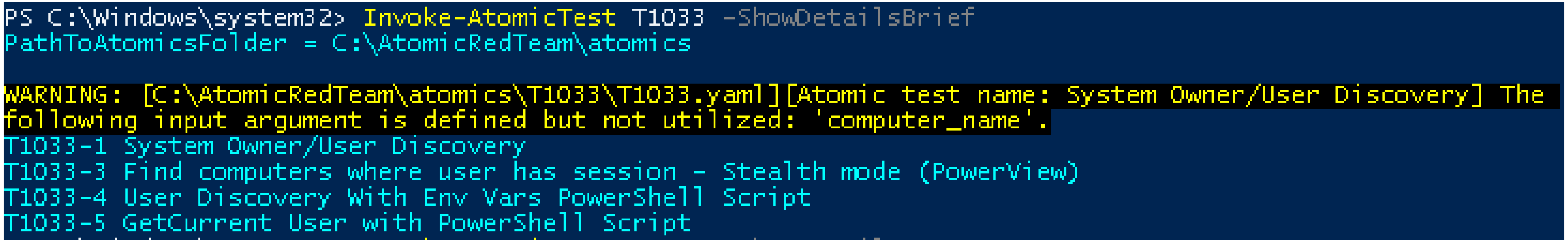


```
PS C:\Windows\system32> IEX (IWR 'https://raw.githubusercontent.com
/redcanaryco/invoke-atomicredteam/master/install-atomicredteam.ps1'
 -UseBasicParsing); -getAtomics_
```



```
PS C:\Windows\system32> Install-Module -Name invoke-atomicredteam,
powershell-yaml -Scope CurrentUser_
```

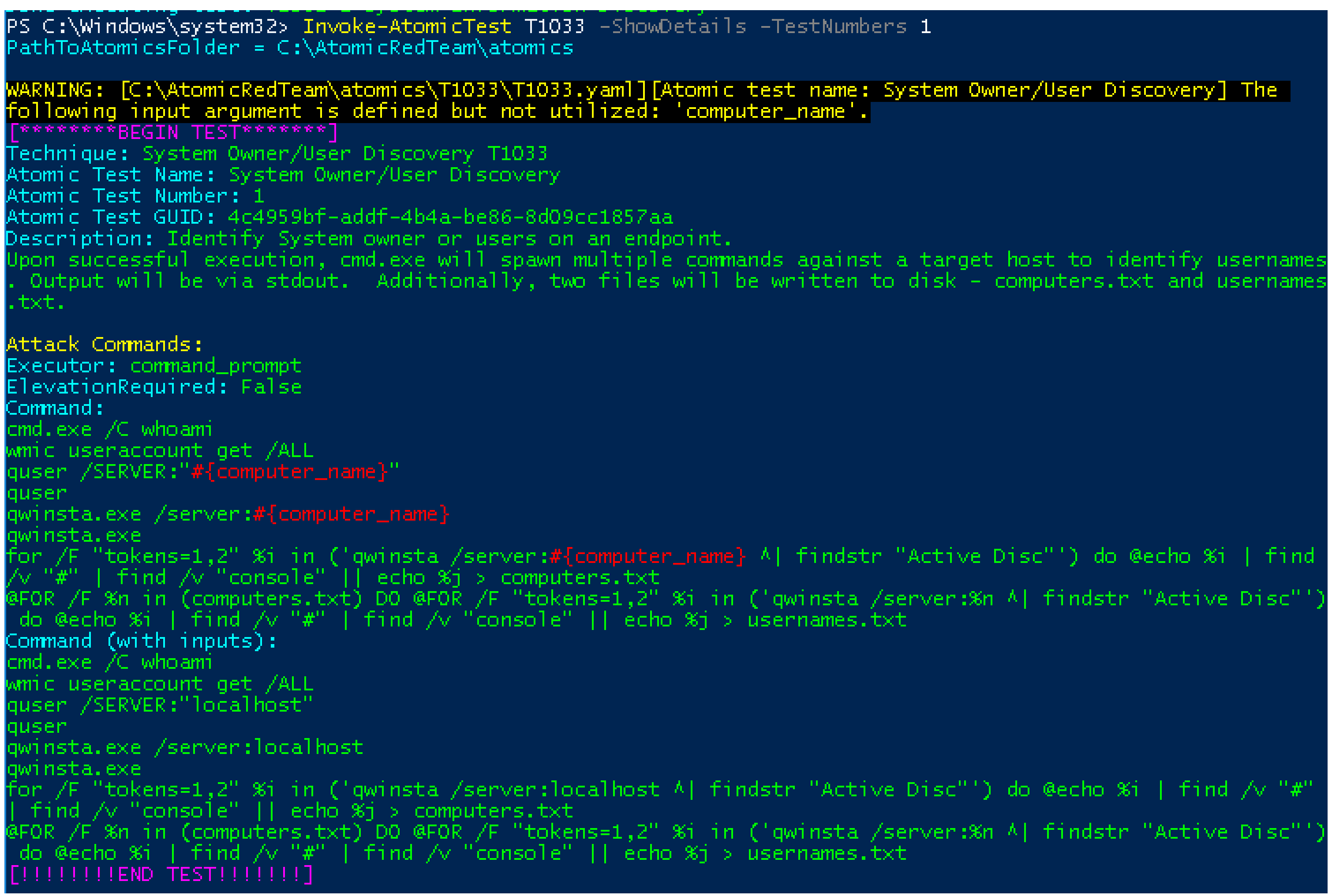
DEMONSTRATION



```
PS C:\Windows\system32> Invoke-AtomicTest T1033 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

WARNING: [C:\AtomicRedTeam\atomics\T1033\T1033.yaml][Atomic test name: System Owner/User Discovery] The
following input argument is defined but not utilized: 'computer_name'.
T1033-1 System Owner/User Discovery
T1033-3 Find computers where user has session - Stealth mode (PowerView)
T1033-4 User Discovery With Env Vars PowerShell Script
T1033-5 GetCurrent User with PowerShell Script
```

DEMONSTRATION

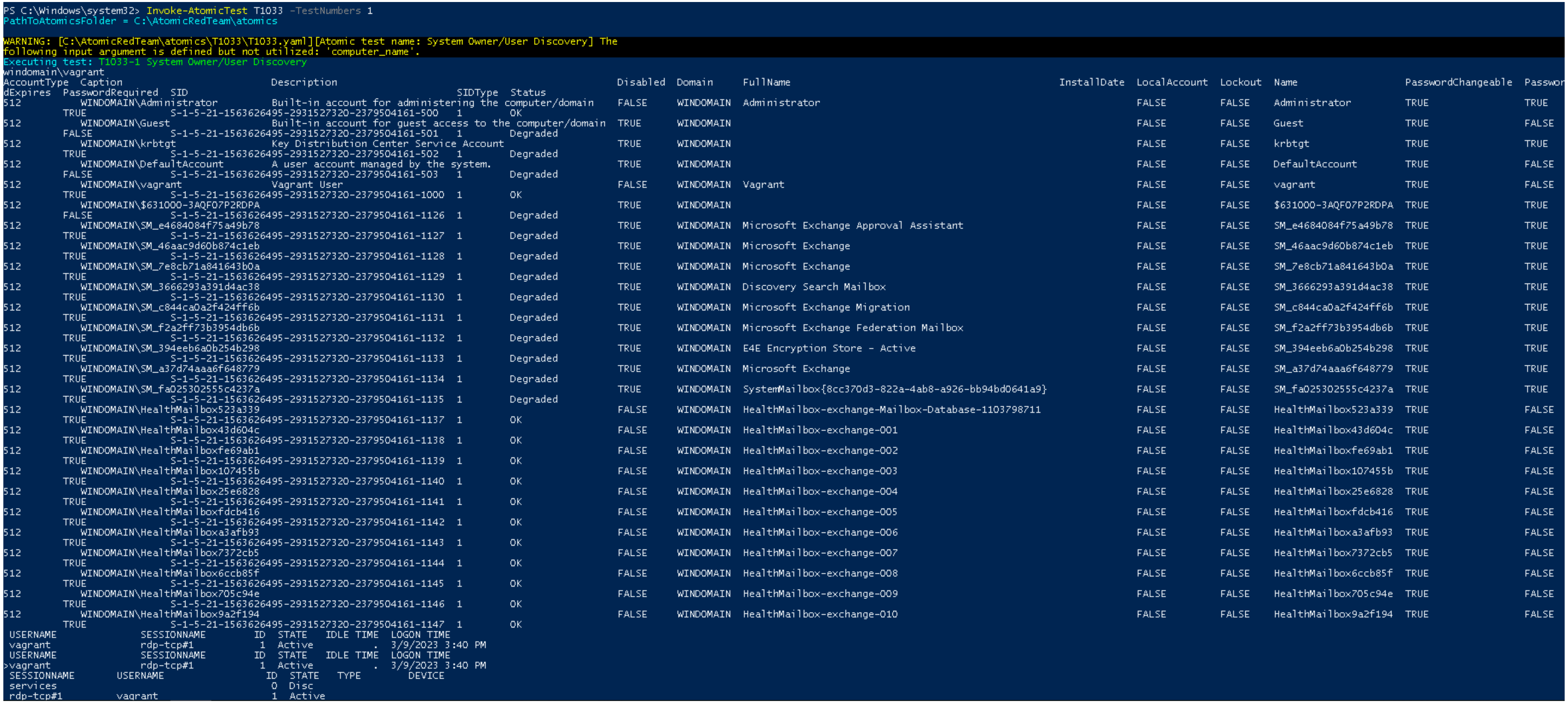


```
PS C:\Windows\system32> Invoke-AtomicTest T1033 -ShowDetails -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

WARNING: [C:\AtomicRedTeam\atomics\T1033\T1033.yaml][Atomic test name: System Owner/User Discovery] The
following input argument is defined but not utilized: 'computer_name'.
[********BEGIN TEST*******]
Technique: System Owner/User Discovery T1033
Atomic Test Name: System Owner/User Discovery
Atomic Test Number: 1
Atomic Test GUID: 4c4959bf-addf-4b4a-be86-8d09cc1857aa
Description: Identify System owner or users on an endpoint.
Upon successful execution, cmd.exe will spawn multiple commands against a target host to identify usernames
. Output will be via stdout.  Additionally, two files will be written to disk - computers.txt and usernames
.txt.

Attack Commands:
Executor: command_prompt
ElevationRequired: False
Command:
cmd.exe /C whoami
wmic useraccount get /ALL
quser /SERVER:"#{computer_name}"
quser
qwinsta.exe /server:#{computer_name}
qwinsta.exe
for /F "tokens=1,2" %i in ('qwinsta /server:#{computer_name} ^| findstr "Active Disc"') do @echo %i | find
/v "#" | find /v "console" || echo %j > computers.txt
@FOR /F %n in (computers.txt) DO @FOR /F "tokens=1,2" %i in ('qwinsta /server:%n ^| findstr "Active Disc")
 do @echo %i | find /v "#" | find /v "console" || echo %j > usernames.txt
Command (with inputs):
cmd.exe /C whoami
wmic useraccount get /ALL
quser /SERVER:"localhost"
quser
qwinsta.exe /server:localhost
qwinsta.exe
for /F "tokens=1,2" %i in ('qwinsta /server:localhost ^| findstr "Active Disc"') do @echo %i | find /v "#"
| find /v "console" || echo %j > computers.txt
@FOR /F %n in (computers.txt) DO @FOR /F "tokens=1,2" %i in ('qwinsta /server:%n ^| findstr "Active Disc")
 do @echo %i | find /v "#" | find /v "console" || echo %j > usernames.txt
[!!!!!!!!END TEST!!!!!!!]
```

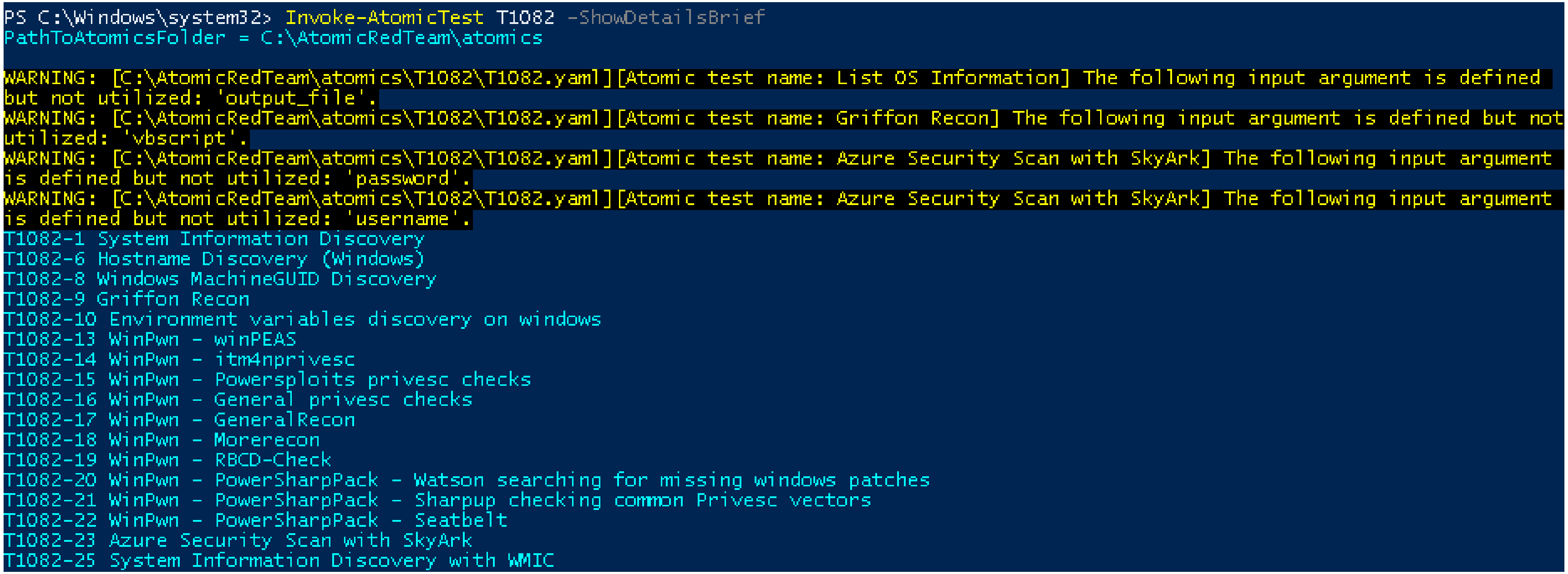
DEMONSTRATION



```
PS C:\Windows\system32> Invoke-AtomicTest T1033 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

WARNING: [C:\AtomicRedTeam\atomics\T1033\T1033.yaml][Atomic test name: System Owner/User Discovery] The
following input argument is defined but not utilized: 'computer_name'.
Executing test: T1033-1 System Owner/User Discovery
windomain\vagrant
AccountType  Caption                         Description                                               Disabled  Domain     FullName                                             InstallDate  LocalAccount  Lockout  Name                  PasswordChangeable  Passwor
dExpires  PasswordRequired  SID                                             SIDType  Status
512          WINDOMAIN\Administrator         Built-in account for administering the computer/domain    FALSE     WINDOMAIN  Administrator                                                     FALSE         FALSE    Administrator         TRUE                TRUE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-500   1        OK
512          WINDOMAIN\Guest                 Built-in account for guest access to the computer/domain  TRUE      WINDOMAIN                                                                    FALSE         FALSE    Guest                 TRUE                FALSE
          FALSE             S-1-5-21-1563626495-2931527320-2379504161-501   1        Degraded
512          WINDOMAIN\krbtgt                Key Distribution Center Service Account                   TRUE      WINDOMAIN                                                                    FALSE         FALSE    krbtgt                TRUE                TRUE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-502   1        Degraded
512          WINDOMAIN\DefaultAccount        A user account managed by the system.                     TRUE      WINDOMAIN                                                                    FALSE         FALSE    DefaultAccount        TRUE                FALSE
          FALSE             S-1-5-21-1563626495-2931527320-2379504161-503   1        Degraded
512          WINDOMAIN\vagrant               Vagrant User                                              FALSE     WINDOMAIN  Vagrant                                                           FALSE         FALSE    vagrant               TRUE                FALSE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1000  1        OK
512          WINDOMAIN\$631000-3AQF07P2RDPA                                                            TRUE      WINDOMAIN                                                                    FALSE         FALSE    $631000-3AQF07P2RDPA  TRUE                TRUE
          FALSE             S-1-5-21-1563626495-2931527320-2379504161-1126  1        Degraded
512          WINDOMAIN\SM_e4684084f75a49b78                                                            TRUE      WINDOMAIN  Microsoft Exchange Approval Assistant                             FALSE         FALSE    SM_e4684084f75a49b78  TRUE                TRUE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1127  1        Degraded
512          WINDOMAIN\SM_46aac9d60b874c1eb                                                            TRUE      WINDOMAIN  Microsoft Exchange                                                FALSE         FALSE    SM_46aac9d60b874c1eb  TRUE                TRUE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1128  1        Degraded
512          WINDOMAIN\SM_7e8cb71a841643b0a                                                            TRUE      WINDOMAIN  Microsoft Exchange                                                FALSE         FALSE    SM_7e8cb71a841643b0a  TRUE                TRUE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1129  1        Degraded
512          WINDOMAIN\SM_3666293a391d4ac38                                                            TRUE      WINDOMAIN  Discovery Search Mailbox                                          FALSE         FALSE    SM_3666293a391d4ac38  TRUE                TRUE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1130  1        Degraded
512          WINDOMAIN\SM_c844ca0a2f424ff6b                                                            TRUE      WINDOMAIN  Microsoft Exchange Migration                                      FALSE         FALSE    SM_c844ca0a2f424ff6b  TRUE                TRUE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1131  1        Degraded
512          WINDOMAIN\SM_f2a2ff73b3954db6b                                                            TRUE      WINDOMAIN  Microsoft Exchange Federation Mailbox                             FALSE         FALSE    SM_f2a2ff73b3954db6b  TRUE                TRUE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1132  1        Degraded
512          WINDOMAIN\SM_394eeb6a0b254b298                                                            TRUE      WINDOMAIN  E4E Encryption Store - Active                                     FALSE         FALSE    SM_394eeb6a0b254b298  TRUE                TRUE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1133  1        Degraded
512          WINDOMAIN\SM_a37d74aaa6f648779                                                            TRUE      WINDOMAIN  Microsoft Exchange                                                FALSE         FALSE    SM_a37d74aaa6f648779  TRUE                TRUE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1134  1        Degraded
512          WINDOMAIN\SM_fa025302555c4237a                                                            TRUE      WINDOMAIN  SystemMailbox{8cc370d3-822a-4ab8-a926-bb94bd0641a9}               FALSE         FALSE    SM_fa025302555c4237a  TRUE                TRUE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1135  1        Degraded
512          WINDOMAIN\HealthMailbox523a339                                                            FALSE     WINDOMAIN  HealthMailbox-exchange-Mailbox-Database-1103798711                FALSE         FALSE    HealthMailbox523a339  TRUE                FALSE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1137  1        OK
512          WINDOMAIN\HealthMailbox43d604c                                                            FALSE     WINDOMAIN  HealthMailbox-exchange-001                                        FALSE         FALSE    HealthMailbox43d604c  TRUE                FALSE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1138  1        OK
512          WINDOMAIN\HealthMailboxfe69ab1                                                            FALSE     WINDOMAIN  HealthMailbox-exchange-002                                        FALSE         FALSE    HealthMailboxfe69ab1  TRUE                FALSE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1139  1        OK
512          WINDOMAIN\HealthMailbox107455b                                                            FALSE     WINDOMAIN  HealthMailbox-exchange-003                                        FALSE         FALSE    HealthMailbox107455b  TRUE                FALSE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1140  1        OK
512          WINDOMAIN\HealthMailbox25e6828                                                            FALSE     WINDOMAIN  HealthMailbox-exchange-004                                        FALSE         FALSE    HealthMailbox25e6828  TRUE                FALSE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1141  1        OK
512          WINDOMAIN\HealthMailboxfdcb416                                                            FALSE     WINDOMAIN  HealthMailbox-exchange-005                                        FALSE         FALSE    HealthMailboxfdcb416  TRUE                FALSE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1142  1        OK
512          WINDOMAIN\HealthMailboxa3afb93                                                            FALSE     WINDOMAIN  HealthMailbox-exchange-006                                        FALSE         FALSE    HealthMailboxa3afb93  TRUE                FALSE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1143  1        OK
512          WINDOMAIN\HealthMailbox7372cb5                                                            FALSE     WINDOMAIN  HealthMailbox-exchange-007                                        FALSE         FALSE    HealthMailbox7372cb5  TRUE                FALSE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1144  1        OK
512          WINDOMAIN\HealthMailbox6ccb85f                                                            FALSE     WINDOMAIN  HealthMailbox-exchange-008                                        FALSE         FALSE    HealthMailbox6ccb85f  TRUE                FALSE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1145  1        OK
512          WINDOMAIN\HealthMailbox705c94e                                                            FALSE     WINDOMAIN  HealthMailbox-exchange-009                                        FALSE         FALSE    HealthMailbox705c94e  TRUE                FALSE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1146  1        OK
512          WINDOMAIN\HealthMailbox9a2f194                                                            FALSE     WINDOMAIN  HealthMailbox-exchange-010                                        FALSE         FALSE    HealthMailbox9a2f194  TRUE                FALSE
          TRUE              S-1-5-21-1563626495-2931527320-2379504161-1147  1        OK
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
 vagrant               rdp-tcp#1           1  Active          .  3/9/2023 3:40 PM
 USERNAME              SESSIONNAME        ID  STATE   IDLE TIME  LOGON TIME
>vagrant               rdp-tcp#1           1  Active          .  3/9/2023 3:40 PM
 SESSIONNAME       USERNAME                 ID  STATE   TYPE        DEVICE
 services                                    0  Disc
 rdp-tcp#1         vagrant                   1  Active
```

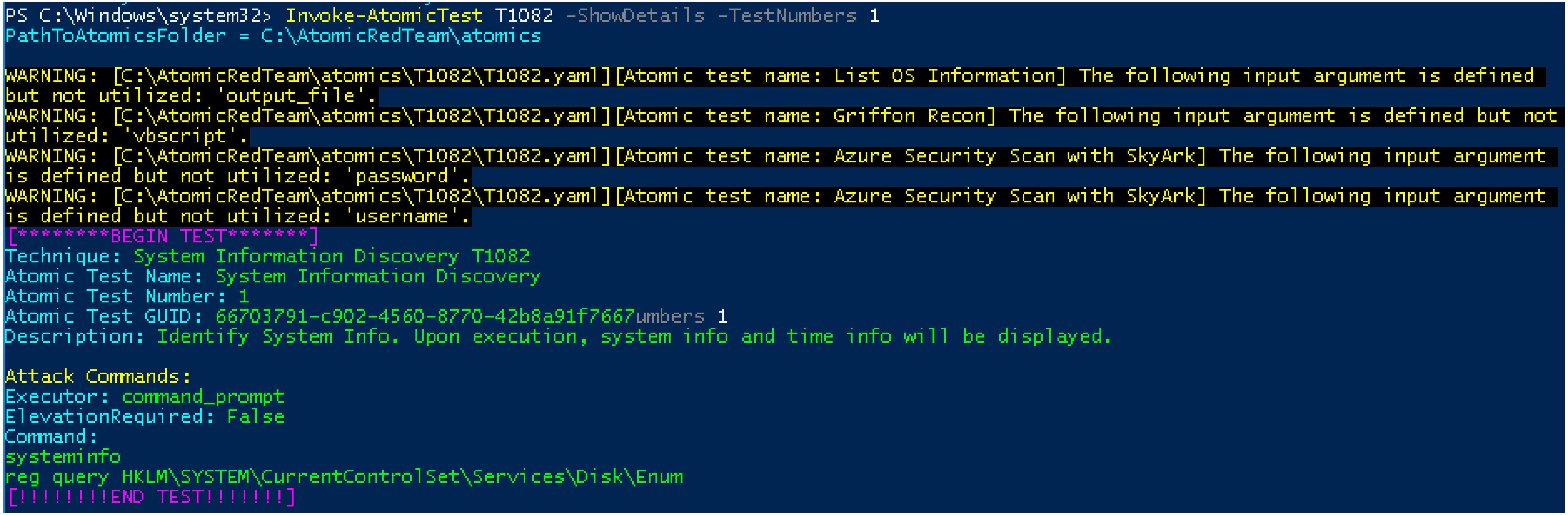
DEMONSTRATION



```
PS C:\Windows\system32> Invoke-AtomicTest T1082 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

WARNING: [C:\AtomicRedTeam\atomics\T1082\T1082.yaml][Atomic test name: List OS Information] The following input argument is defined
but not utilized: 'output_file'.
WARNING: [C:\AtomicRedTeam\atomics\T1082\T1082.yaml][Atomic test name: Griffon Recon] The following input argument is defined but not
utilized: 'vbscript'.
WARNING: [C:\AtomicRedTeam\atomics\T1082\T1082.yaml][Atomic test name: Azure Security Scan with SkyArk] The following input argument
is defined but not utilized: 'password'.
WARNING: [C:\AtomicRedTeam\atomics\T1082\T1082.yaml][Atomic test name: Azure Security Scan with SkyArk] The following input argument
is defined but not utilized: 'username'.
T1082-1 System Information Discovery
T1082-6 Hostname Discovery (Windows)
T1082-8 Windows MachineGUID Discovery
T1082-9 Griffon Recon
T1082-10 Environment variables discovery on windows
T1082-13 WinPwn - winPEAS
T1082-14 WinPwn - itm4nprivesc
T1082-15 WinPwn - Powersploits privesc checks
T1082-16 WinPwn - General privesc checks
T1082-17 WinPwn - GeneralRecon
T1082-18 WinPwn - Morerecon
T1082-19 WinPwn - RBCD-Check
T1082-20 WinPwn - PowerSharpPack - Watson searching for missing windows patches
T1082-21 WinPwn - PowerSharpPack - Sharpup checking common Privesc vectors
T1082-22 WinPwn - PowerSharpPack - Seatbelt
T1082-23 Azure Security Scan with SkyArk
T1082-25 System Information Discovery with WMIC
```

DEMONSTRATION

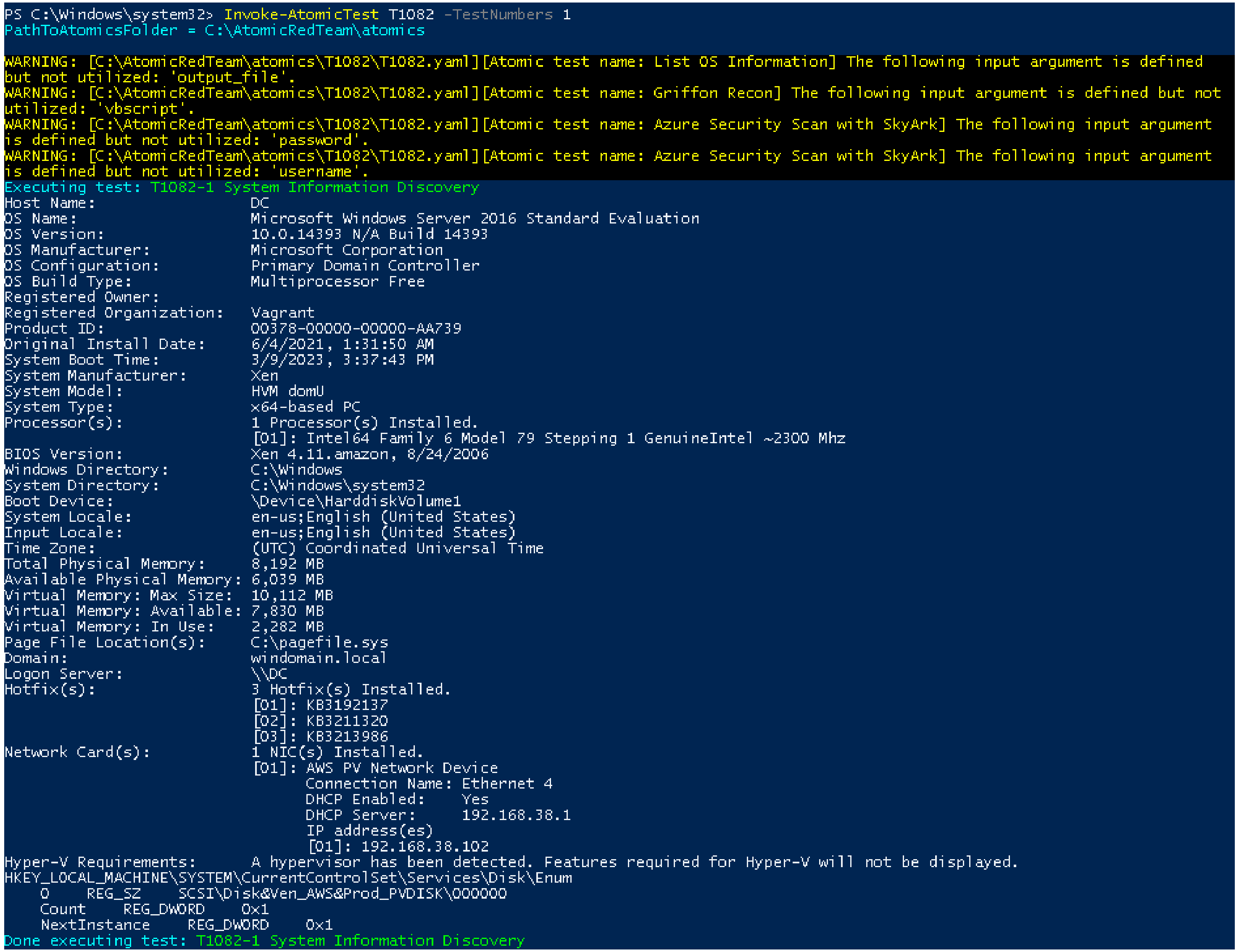


```
PS C:\Windows\system32> Invoke-AtomicTest T1082 -ShowDetails -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

WARNING: [C:\AtomicRedTeam\atomics\T1082\T1082.yaml][Atomic test name: List OS Information] The following input argument is defined
but not utilized: 'output_file'.
WARNING: [C:\AtomicRedTeam\atomics\T1082\T1082.yaml][Atomic test name: Griffon Recon] The following input argument is defined but not
utilized: 'vbscript'.
WARNING: [C:\AtomicRedTeam\atomics\T1082\T1082.yaml][Atomic test name: Azure Security Scan with SkyArk] The following input argument
is defined but not utilized: 'password'.
WARNING: [C:\AtomicRedTeam\atomics\T1082\T1082.yaml][Atomic test name: Azure Security Scan with SkyArk] The following input argument
is defined but not utilized: 'username'.
[********BEGIN TEST*******]
Technique: System Information Discovery T1082
Atomic Test Name: System Information Discovery
Atomic Test Number: 1
Atomic Test GUID: 66703791-c902-4560-8770-42b8a91f7667umbers 1
Description: Identify System Info. Upon execution, system info and time info will be displayed.

Attack Commands:
Executor: command_prompt
ElevationRequired: False
Command:
systeminfo
reg query HKLM\SYSTEM\CurrentControlSet\Services\Disk\Enum
[!!!!!!!!END TEST!!!!!!!]
```

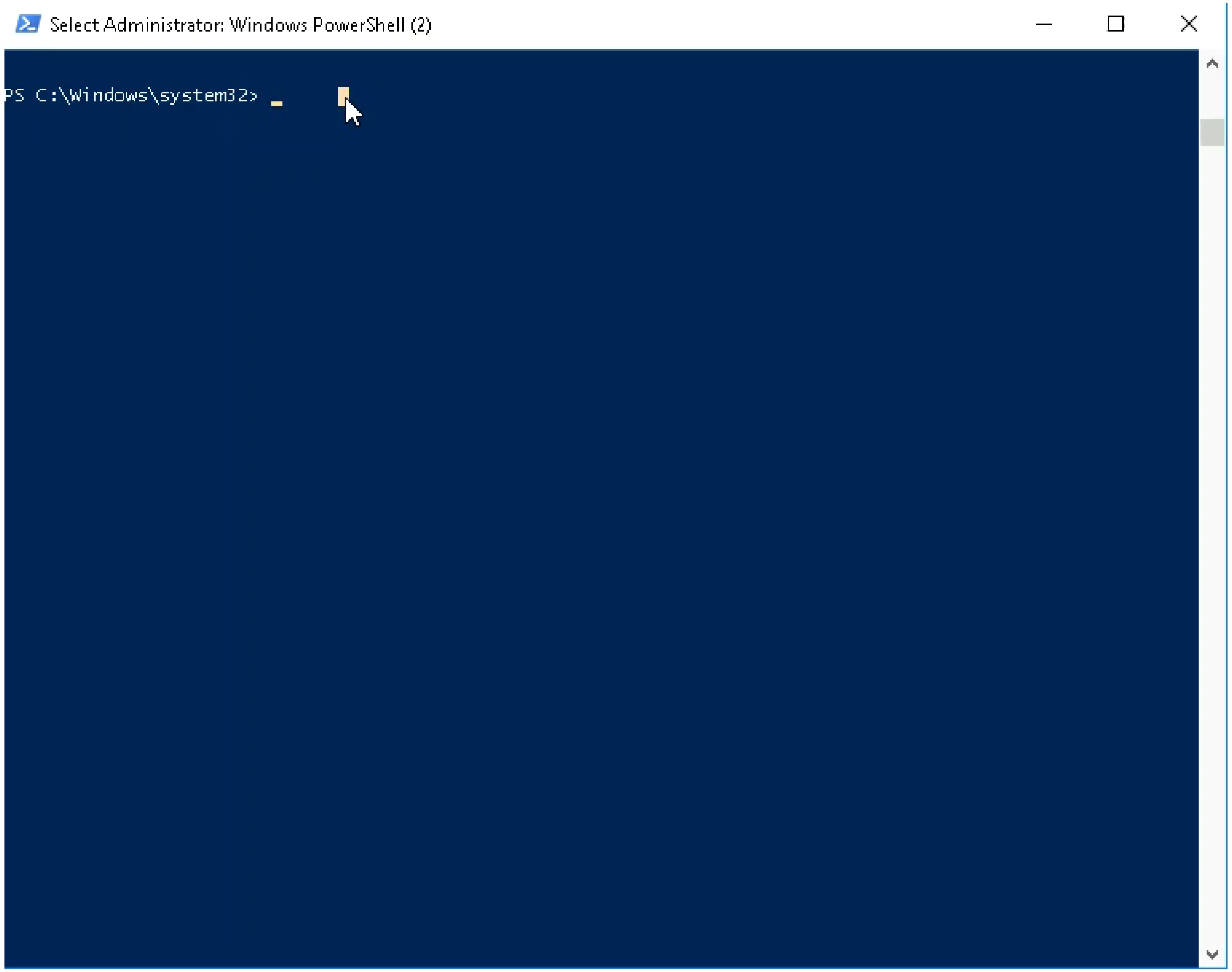
DEMONSTRATION



```
PS C:\Windows\system32> Invoke-AtomicTest T1082 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

WARNING: [C:\AtomicRedTeam\atomics\T1082\T1082.yaml][Atomic test name: List OS Information] The following input argument is defined
but not utilized: 'output_file'.
WARNING: [C:\AtomicRedTeam\atomics\T1082\T1082.yaml][Atomic test name: Griffon Recon] The following input argument is defined but not
utilized: 'vbscript'.
WARNING: [C:\AtomicRedTeam\atomics\T1082\T1082.yaml][Atomic test name: Azure Security Scan with SkyArk] The following input argument
is defined but not utilized: 'password'.
WARNING: [C:\AtomicRedTeam\atomics\T1082\T1082.yaml][Atomic test name: Azure Security Scan with SkyArk] The following input argument
is defined but not utilized: 'username'.
Executing test: T1082-1 System Information Discovery
Host Name:                 DC
OS Name:                   Microsoft Windows Server 2016 Standard Evaluation
OS Version:                10.0.14393 N/A Build 14393
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Primary Domain Controller
OS Build Type:             Multiprocessor Free
Registered Owner:
Registered Organization:   Vagrant
Product ID:                00378-00000-00000-AA739
Original Install Date:     6/4/2021, 1:31:50 AM
System Boot Time:          3/9/2023, 3:37:43 PM
System Manufacturer:       Xen
System Model:              HVM domU
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 79 Stepping 1 GenuineIntel ~2300 Mhz
BIOS Version:              Xen 4.11.amazon, 8/24/2006
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (UTC) Coordinated Universal Time
Total Physical Memory:     8,192 MB
Available Physical Memory: 6,039 MB
Virtual Memory: Max Size:  10,112 MB
Virtual Memory: Available: 7,830 MB
Virtual Memory: In Use:    2,282 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    windomain.local
Logon Server:              \\DC
Hotfix(s):                 3 Hotfix(s) Installed.
                           [01]: KB3192137
                           [02]: KB3211320
                           [03]: KB3213986
Network Card(s):           1 NIC(s) Installed.
                           [01]: AWS PV Network Device
                                 Connection Name: Ethernet 4
                                 DHCP Enabled:    Yes
                                 DHCP Server:     192.168.38.1
                                 IP address(es)
                                 [01]: 192.168.38.102
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will not be displayed.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Disk\Enum
    0    REG_SZ    SCSI\Disk&Ven_AWS&Prod_PVDISK\000000
    Count    REG_DWORD    0x1
    NextInstance    REG_DWORD    0x1
Done executing test: T1082-1 System Information Discovery
```

DEMONSTRATION



```
PS C:\Windows\system32> _
```

QUESTIONS?

LET'S CONNECT!

RITA L. GRIFFITH CISA, CFE

Senior Manager, IT Assurance

RGriffith@wolfandco.com

617.261.8185

LET'S CONNECT!

SEAN D. GOODWIN, GSE

Senior Manager, DenSecure

SDGoodwin@wolfandco.com

617.261.8139

ABOUT WOLF & COMPANY, P.C.

1911 WOLF & CO. ESTABLISHED

300+ PROFESSIONALS

3 OFFICES IN:

- Boston, MA
- Springfield, MA
- Princeton, NJ

SERVICES OFFERED IN:

- Audit
- Tax
- Risk Management

ABOUT WOLF & COMPANY, P.C.

111

YEARS IN BUSINESS

- ✓ Established in 1911
- ✓ Built on quality and integrity
- ✓ Succession strategy to remain independent allows us to be with you throughout your business lifecycle

300+

EXPERIENCED, HIGHLY TRAINED PROFESSIONALS

- ✓ Lower-than-industry-average staff turnover means a consistent team structure year after year
- ✓ Niche team dedicated to your industry

RESOURCES TO LEARN MORE

- ✓ Cultures & Values
- ✓ Inclusion & Diversity
- ✓ Our History
- ✓ Social Responsibility
- ✓ Thought Leadership
- ✓ Wolf Global

Wolf & Company ranked

#2 BEST LARGE FIRM TO WORK FOR

nationwide

accountingTODAY

WOLF & COMPANY, P.C.

den secure by wolf & company, p.c.

SERVICES WE OFFER

We combine industry expertise with service specialization to provide your organization with insight, opportunities, and solutions allowing you to address your unique business needs.

ADVISORY

- Business Continuity Planning
- Cybersecurity
- Data Analytics & Management
- Digital Transformation
- Enterprise Risk Management
- Environment, Social & Governance
- Internal Audit
- IT Audit
- Model Risk Management
- Outsourced Accounting Solutions
- Regulatory Compliance
- Strategic Planning

ASSURANCE

- Employee Benefit Plan Audits
- Financial Statements Audits
- HITRUST
- PCI DSS
- SOC Reporting

TAX

- Business Tax
- Federal
- International
- State & Local
- Private Client Group

vSUITE

Virtual risk management consulting services

- Virtual Chief Information Security Officer (vCISO)
- Virtual Chief Privacy Officer (vCPO)
- Virtual Chief Risk Officer (vCRO)
- Virtual Vendor Management

WOLFPAC

Integrated risk management SaaS suite

DENSECURE

Advanced cyber threat experts

WOLF & COMPANY, P.C.

densecure by wolf & company, p.c.

WOLF ACCOLADES

Wolf is pleased to have received recognition from a variety of sources for our efforts at providing responsive client service and development of our professionals. Examples of this recognition include:

INSIDE Public Accounting

TOP 100
Accounting Firms

accountingTODAY

TOP 100
Accounting Firms

#2 BEST LARGE FIRM to
Work For Nationwide

TOP FIRMS:
New England

BOSTON
BUSINESS JOURNAL

- ✓ Area's Best Places to Work
- ✓ Area's Most Admired Companies
- ✓ Area's Fastest Growing Private Companies
- ✓ Area's Largest I.T. Consulting Firms

Forbes

America's Best
Tax and Accounting
Firms of 2023, 2021

ABOUT DENSECURE

Wolf & Company's IT Assurance & Advisory team of cybersecurity experts, DenSecure™, brings together extensive technical knowledge and industry experience with internationally-recognized frameworks to develop strong cybersecurity programs.

DenSecure's core services include:

- Advanced Security Assessment
- Application Penetration Testing
- Network Penetration Testing
- Social Engineering
- Threat Emulation

Back to Home ⟶